

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<b>(51) International Patent Classification <sup>6</sup> :</b> <b>H04J 13/00</b>	<b>A1</b>	<b>(11) International Publication Number:</b> <b>WO 99/33212</b> <b>(43) International Publication Date:</b> 1 July 1999 (01.07.99)
<b>(21) International Application Number:</b> PCT/IE98/00110 <b>(22) International Filing Date:</b> 18 December 1998 (18.12.98) <b>(30) Priority Data:</b> S970900 19 December 1997 (19.12.97) IE <b>(71) Applicant (for all designated States except US):</b> SUPERGOLD COMMUNICATION LIMITED [IE/IE]; Molesworth House, 1 South Frederick Street, Dublin 2 (IE). <b>(72) Inventor; and</b> <b>(75) Inventor/Applicant (for US only):</b> O'FARRELL, Timothy [GB/GB]; 33 Crosters Lea, Yeadon, Leeds LS19 7WE (GB). <b>(74) Agent:</b> MACLACHLAN & DONALDSON; 47 Merrion Square, Dublin 2 (IE).		<b>(81) Designated States:</b> AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).  <b>Published</b> <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>
<b>(54) Title:</b> CONCATENATED CODES FOR SPREAD SPECTRUM COMMUNICATION  <b>(57) Abstract</b> <p>Spread spectrum communication techniques and applications using signature sequences are described to reduce the effects of certain transmission impairments such as co-channel interference, multiple access interference and intersymbol interference. Signature sequences with structured properties are obtained by generating cosets from a seed set of sequences, constructing a subset of sequences by concatenating the sequences of a coset and constructing a full set of sequences by concatenating the subsets of sequences.</p>		

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

## CONCATENATED CODES FOR SPREAD SPECTRUM COMMUNICATION

The present invention relates to spread spectrum communication and more particularly, to spread spectrum communication techniques and applications using signature sequences.

5

Spread spectrum communication techniques are used for information carrying signals in a variety of communication systems because of their ability to reduce the effects of certain transmission impairments. Many multi-user communication techniques suffer co-channel interference, multiple access interference and intersymbol interference. The use of spread spectrum transmission and reception attenuates these interference types.

10

In Local Area Networks (LANs) there is an increasing desire to extend or replace wired LANs in order to increase functionality and maximise the number of potential applications for such systems. This trend facilitates the growing need for wireless access. This wireless access allows mobile computer users to remain in contact with a given corporate LAN over short distances. Currently available systems provide such connections using either radio or infrared communication technology. For certain system requirements, this communication is adequate. However, the application of such technologies to wireless LANs is relatively new and therefore can prove to be both expensive and unreliable. Furthermore, the data transmission rates achievable are relatively low which significantly limits the number of applications to which the systems may be applied. Coverage of a large area using infrared technology is particularly expensive, even more expensive than the radio communication equivalent. While point-to-point or line-of-sight infrared technology is cheaper than radio technology, it is unsuitable for most wireless LANs.

15

20

25

The main constraint on using any wireless LAN is interference. Infrared transmission particularly suffers from inter-symbol interference produced by multipath propagation effects. Achieving full coverage in an operating environment, while keeping within the limits of eye safety presents another problem to system designers, as does contending with interference produced by natural and man-made light sources that might be present. A further problem occurs when designing infrared receivers for such systems in that the receivers must provide the required sensitivity and bandwidth at minimal cost.

30

- 2 -

Achieving full room coverage while avoiding multipath propagation are conflicting requirements in a wireless infrared LAN and full room coverage is essential if reliable communication to and from any point within the room is needed. In order to achieve full room coverage, it is necessary to diffuse the transmitted infrared radiation. While diffuse transmission will reflect off walls and ceilings to fill the room the signal power reaching a given receiver is usually very small necessitating the use of very sensitive receivers. The problem of sensitivity is compounded by the necessity to detect a weak information bearing signal in strong interference. As a result of these problems there are few commercial infrared wireless LANs or associated systems available on the market.

Commercially available systems therefore tend to use elaborate structures and circuitry, which are expensive when compared with radio technologies. While there is a dearth of infrared technologies that support multi-user communication, there are numerous infrared technologies that support directed line-of-sight transmission. The most commonly available of these is the infrared serial port link based on the Infrared Data Association (IrDA) Standard. IrDA links can operate at data rates up to 4 Mb/s and are used in relatively inexpensive IrDA access points. However, IrDA links are only guaranteed to operate over a one metre range and are limited generally to one-to-one communication. IrDA is primarily intended as a replacement for a single wire-connection and is not intended for multi-user access. Notwithstanding this limitation, the popularity of IrDA clearly illustrates the enormous demand for reliable wireless technology. The best way to achieve multi-user links is to flood the operating environment with infrared light. While this enables multiple-users to connect to a network from anywhere in the operating environment, significant power is lost in such a diffuse environment thereby compromising the signal-to-noise ratio (SNR) at the receiver.

It is an object of the present invention to seek to provide a method and apparatus for the generation of signature sequences for spread spectrum communication, which will overcome the aforementioned problems. It is a further object of the invention to provide transmitter and receiver circuitry for coded spread spectrum signals.

- 3 -

Accordingly, the present invention provides a method of constructing signature sequences for spread spectrum communication techniques, the method comprising:

- selecting a seed set of sequences;
- 5 forming cosets from the seed set of sequences;
- constructing a subset of sequences by concatenating the sequences of a coset; and
- 10 constructing a full set of sequences by concatenating subsets of sequences.

The invention further provides an apparatus for constructing and encoding signature sequences for spread spectrum communication techniques, the apparatus comprising:

- 15 a seed set generating means for constructing a seed set of sequences;
- a coset generating means for generating cosets of sequences;
- an expansion means which concatenates the sequences of a coset according to a
- 20 predetermined order to form a subset of sequences for each coset; and
- a set generating means for constructing a full set of sequences by concatenating subsets.

- 25 Conveniently, the seed set generating means comprises a plurality of shift registers each having an input, a system clock input, logic gates, a plurality of register cells/stages and an output to form a sequence of the seed set. A typical seed set generating means is constructed from a number of linear feedback shift registers.

- 30 The cosets are formed from the seed set utilising biphase multiplication techniques, preferably by multiplication of each sequence of the seed set by a sequence element for each element of the corresponding sequence.

- 4 -

The expansion means comprises a plurality of inputs, each one corresponding to a sequence from a coset, multiplexers, counters, logic gates, a system clock input and a plurality of outputs to form a subset of sequences.

- 5 The set generating means comprises a plurality of shift registers each having an input, a system clock input and a plurality of register cells/stages with outputs to form the full set of sequences.

10 Preferably, the seed set generating means, the coset generating means, the expansion means and the full set generating means are realisable utilising electronic circuitry, including memory devices such as registers, ASICs or FPLAs. Optionally, the means are realisable utilising dedicated software techniques.

15 The present invention also provides an apparatus for decoding signature sequences in a spread spectrum communications system, the apparatus comprising:

means for receiving coded signals;

20 means for generating sequence functions;

means for combining received coded signals with sequence functions to produce despread signal outputs;

25 means for combining the despread signal outputs to generate a data stream; and  
logic circuitry for analysing the data stream.

30 The invention yet further provides transmitter and receiver circuits including the encoding and decoding apparatus described hereinabove, respectively, each circuit being adapted for use with the signature sequences of the present invention.

- 5 -

In a first exemplifying embodiment, an infrared communications system for a wireless local area network comprises a plurality of remote communication terminals, each terminal including a transmitter circuit having means for generating and encoding signature sequences for spread spectrum communication techniques, a means for transmitting coded infrared signals and a receiver circuit for receiving coded infrared signals having means for decoding signature sequences in a spread spectrum communication system.

In a second exemplifying embodiment, a radio communication system for a wireless local area network comprises a plurality of remote communication terminals, each terminal including a transmitter circuit having means for generating and encoding signature sequences for spread spectrum communication techniques, a means for transmitting coded radio signals and a receiver circuit for receiving coded radio signals having means for decoding signature sequences in a spread spectrum communication system.

In a third exemplifying embodiment, a radio code division multiple access (CDMA) communication system for use, for example, in cellular mobile radio networks, wireless local loop networks, radio packet data networks or satellite networks comprises a plurality of remote communication terminals that send and receive radio signals to and from, respectively, a central base station. Each base station has transmitter circuits having means for generating and encoding signature sequences for CDMA communication techniques, a means for transmitting coded radio signals and receiver circuits for receiving coded radio signals having means for decoding signature sequences in a radio CDMA communication system. Each remote terminal has a transmitter circuit having means for generating and encoding signature sequences for CDMA communication techniques, a means for transmitting coded radio signals and a receiver circuit for receiving coded radio signals having means for decoding signature sequences in a CDMA communication system.

In a fourth exemplifying embodiment, a lightwave CDMA communication system for an optical fibre local area network comprises a plurality of remote communication terminals that transmit and receive lightwave signals and which are interconnected by optical fibre. Each terminal has a transmitter circuit having means for generating and encoding signature sequences for lightwave CDMA communication techniques, a means for transmitting

- 6 -

coded lightwave signals and a receiver circuit for receiving a coded lightwave signals having means for decoding signature sequences in a lightwave CDMA communication system.

- 5     The term "lightwave" is taken to mean electromagnetic radiation within the ranges of visible light and near and far infrared light.

According to one aspect of the invention there is provided a method for spread spectrum communication using a signature sequence, the signature sequence being generated by  
10   performing the steps of:-

selecting a seed set of sequences of a given size;

generating a plurality of cosets from the seed set of sequences;

15

constructing a subset of sequences by concatenating the sequences of a coset; and

constructing a full set of sequences by concatenating subsets of sequences.

- 20   Preferably, the seed set contains binary sequences.

Preferably, the binary sequence is cyclically distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition.

- 25   In one arrangement, the seed set contains complex sequences.

Preferably, the seed set incorporates a plurality of inner sequences.

Preferably, the seed set is orthogonal.

30

Ideally, the cosets are generated by multiplying in turn each inner sequence by an element of an associated sequence.



- 7 -

Preferably, the subset of sequences is constructed by concatenating the sequences of a coset using an addition table.

5 In one embodiment of the invention, the addition table is constructed using powers of a primitive root of the seed set of sequences, the primitive root being determined in accordance with the size of the seed set.

10 In another embodiment of the invention, the addition table is constructed using powers of a primitive element of the seed set of sequences, the primitive element being determined in accordance with the size of the seed set.

Preferably, the seed set is formed from a plurality of rotated sequences.

15 According to another aspect of the invention there is provided a method for producing a structured code for use in spread spectrum data communication comprising the steps of:-

selecting a seed set of sequences of a given size;

generating a plurality of cosets from the seed set of sequences;

20

constructing a subset of sequences by concatenating the sequences of a coset; and

constructing a full set of sequences by concatenating subsets of sequences.

25 Preferably, the seed set contains binary sequences.

Preferably, the binary sequence is cyclically distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition.

30 In one arrangement, the seed set contains complex sequences.

Ideally, the seed set incorporates a plurality of inner sequences.

- 8 -

Preferably, the seed set is orthogonal.

In a preferred embodiment, the cosets are generated by multiplying in turn each inner sequence by an element of an associated sequence.

5

Preferably, the subset of sequences is constructed by concatenating the sequences of a coset using an addition table.

10 In one arrangement, the addition table is constructed using powers of a primitive root of the seed set of sequences, the primitive root being determined in accordance with the size of the seed set.

15 In another arrangement, the addition table is constructed using powers of a primitive element of the seed set of sequences, the primitive element being determined in accordance with the size of the seed set.

Preferably, the seed set is formed from a plurality of rotated sequences.

20 According to a further aspect of the invention there is provided an apparatus for constructing and encoding signature sequences for spread spectrum communication techniques, the apparatus comprising:

a seed set generating means for constructing a seed set of sequences;

25 a coset generating means for generating cosets of sequences;

an expansion means for concatenating sequences of a generated coset according to a predetermined order, to form a subset of sequences for each coset; and

30 a set generating means for constructing a full set of sequences by concatenating subsets.

Preferably, the seed set generating means comprises a plurality of shift registers, each shift register having an input, a system clock input, logic gates, a plurality of register cells/stages and an output to form a sequence of the seed set.

5

Preferably, the seed set generating means includes a number of linear feedback shift registers.

In one arrangement, the expansion means comprises:-

10

a plurality of inputs, each input corresponding to a sequence from a coset;

a plurality of multiplexers having associated counters and logic gates;

15

a system clock input; and

a plurality of outputs to form a subset of sequences.

20 Preferably the apparatus is formed for decoding signature sequences in a spread spectrum communications system, the apparatus comprising:

means for receiving coded signals;

25

means for generating sequence functions;

means for combining received coded signals with sequence functions to produce despread signal outputs;

30

means for combining the despread signal outputs to generate a data stream; and

logic circuitry for analysing the data stream.

- 10 -

According to a further aspect of the invention there is provided, a data transmission system having a transmitter and a receiver, the transmitter incorporating means for transmitting data using a signature sequence and the receiver formed for receiving and decoding data  
5 transmitted using a signature sequence, the signature sequence being generated by performing the steps of:-

- selecting a seed set of sequences of a given size;
- 10 generating a plurality of cosets from the seed set of sequences;
- constructing a subset of sequences by concatenating the sequences of a coset; and
- constructing a full set of sequences by concatenating subsets of sequences.

15

According to a still further aspect of the invention there is provided, an electromagnetic radiation or sonic communications system for a communications network comprising a plurality of remote communication terminals, each terminal including a transmitter circuit  
20 having means for generating and encoding signature sequences for spread spectrum communication techniques by performing the steps of selecting a seed set of sequences of a given size, generating a plurality of cosets from the seed set of sequences, constructing a subset of sequences by concatenating the sequences of a coset and constructing a full set of sequences by concatenating subsets of sequences, the transmitter circuit also having, a  
25 means for transmitting coded signals and a receiver circuit for receiving coded signals the receiver circuit having means for decoding signature sequences in a spread spectrum communication system.

Preferably, the communications network uses a radio frequency carrier, an ultrasound  
30 carrier, a seismic carrier or a lightwave or infrared carrier.

Preferably, the receiver circuit incorporates a photodetector, the photodetector having an associated coupling means communicating with a receiver preamplifier.

Preferably, the coupling means is formed for differential signal recognition.

Ideally, the seed set is a balanced seed set.

5

In a preferred arrangement, the encoding signature sequences incorporates orthogonal structured codes.

According to particularly advantageous aspect of the invention there is provided a  
10 communications method for transmission of data in a network using a unipolar-bipolar signaling scheme, the scheme having code division means for separating differential data on a unipolar or bipolar transmission channel.

Preferably, the code division means utilises a binary sequence.

15

Ideally, the binary sequence is orthogonal.

Preferably, the communications method for transmission of data incorporates means for integrating an  $M$ -ary digital transmission scheme based on orthogonal structured codes.

20

The invention will now be described more particularly with reference to the accompanying drawings, which show, by way of example only, communication systems utilising signature sequences in spread spectrum communication techniques according to the invention as exemplified by four embodiments. In the drawings:

25

Figure 1 is a schematic diagram of a transmitter based on  $M$ -ary bi-orthogonal keying for use in a spread spectrum communication system;

Figure 2 is a schematic diagram of a receiver based on  $M$ -ary bi-orthogonal keying for use  
30 in a spread spectrum communication system;

- 12 -

Figure 3 is a schematic diagram of a transmitter based on  $M$ -ary bi-orthogonal keying for use in a wireless infrared spread spectrum communication system;

Figure 4 is a schematic diagram of a receiver based on  $M$ -ary bi-orthogonal keying for use  
5 in a wireless infrared spread spectrum communication system;

Figure 5 is a schematic representation of a differential unipolar-bipolar signaling format;

Figure 6 is a schematic diagram of a transmitter based on  $M$ -ary bi-orthogonal keying and  
10 differential unipolar-bipolar signaling for use in a wireless infrared spread spectrum communication system;

Figure 7 is a schematic diagram of a receiver based on  $M$ -ary bi-orthogonal keying and differential unipolar-bipolar signaling for use in a wireless infrared spread spectrum  
15 communication system;

Figure 8 is a schematic diagram of a transmitter based on  $M$ -ary bi-orthogonal keying and two distinct code sets that can be used in a spread spectrum communication system to double capacity;

20 Figure 9 is a schematic diagram of a receiver based on  $M$ -ary bi-orthogonal keying and two distinct code sets that can be used in a spread spectrum communication system to double capacity;

25 Figure 10 is a schematic representation of a differential unipolar-bipolar signaling format for periodic binary sequences; and

Figure 11 is a chart illustrating some of the applications to which the structured signature sequences of the present invention may advantageously be applied.

30

The method for constructing or generating signature sequences will now be presented. In general, sequence elements may be binary or non-binary, real or complex, quadriphase or

polyphase etc. with corresponding mathematical operations being performed accordingly. In the present disclosure binary sequences are used by way of example. A binary sequence with elements  $\in \{1,0\}$  is mapped into a biphasic sequence with elements  $\in \{-1,1\}$  by using the assignment  $(1 \rightarrow -1)$  and  $(0 \rightarrow 1)$ . Then, modulo-2 addition between binary sequences is achieved by biphasic multiplication between the corresponding biphasic sequences. In order to facilitate explanations, the following notation has been adopted throughout. A biphasic sequence  $\{a_n\}$  has elements  $a_n \in \{-1,1\}$ . However, for simplicity in the description of sequence generation hereinafter, the biphasic notation  $a_n \in \{-,+\}$  is used where symbol "-" refers to "-1" and the symbol "+" refers to "+1". Furthermore, we denote a sequence of length  $w$  by  $\{a_n\} = (a_0, a_1, a_2, \dots, a_{w-1})$  while  $\{a^{(m)}\}$  denotes a set of sequences  $\{a_n^{(0)}\}, \{a_n^{(1)}\}, \{a_n^{(2)}\}, \dots, \{a_n^{(m-1)}\}$  each of length  $w$ . Typically, the sequences belonging to the set  $\{a^{(m)}\}$  are periodic in  $w$ , however, this does not always need to be the case.

New Structured Codes presented hereinafter are a significant development beyond the structured codes described in the prior art. The name Structured Code is a generic name simply referring to the structured nature of these sequences. In the present application, the complete algorithms for constructing Structured Codes are presented for the first time. In addition, specific sets of sequences suitable for spread spectrum systems are presented.

The procedure for constructing a set of Structured Codes is described below. The sequence set  $\{a^{(m)}\}$  specifies a set of  $m$  inner sequences  $\{a_n^{(0)}\}, \{a_n^{(1)}\}, \{a_n^{(2)}\}, \dots, \{a_n^{(m-1)}\}$  each of length  $w$ , where  $m$  is an integer. Then the number of available seed sets is equal to the number of combinations of  $m$  sequences from a total of  $2^w$  sequences (i.e.  $2^w/m!(2^w-m)!$ ) which can be very large. The sequence set  $\{a^{(m)}\}$  is referred to as the seed set and is illustrated below.

$\{a^{(m)}\}$	Seed Set
$\{a_n^{(0)}\}$	$(a_0^{(0)}, a_1^{(0)}, a_2^{(0)}, \dots, a_{w-1}^{(0)})$
$\{a_n^{(1)}\}$	$(a_0^{(1)}, a_1^{(1)}, a_2^{(1)}, \dots, a_{w-1}^{(1)})$
$\{a_n^{(2)}\}$	$(a_0^{(2)}, a_1^{(2)}, a_2^{(2)}, \dots, a_{w-1}^{(2)})$
...	...
$\{a_n^{(m-1)}\}$	$(a_0^{(m-1)}, a_1^{(m-1)}, a_2^{(m-1)}, \dots, a_{w-1}^{(m-1)})$

The seed set  $\{a^{(m)}\}$  is used to construct  $w$  cosets where the  $i$ -th coset, denoted by  $\{c^{(m)}\}_i$  for  $0 \leq i \leq w-1$ , is constructed by multiplying each sequence of  $\{a^{(m)}\}$  by the  $i$ -th element,  $a_i^{(i)}$ , of the corresponding sequence as illustrated below where each coset contains  $m$  sequences each of length  $w$ .

5

$\{c^{(m)}\}_i$	$i$ -th Coset for $0 \leq i \leq w-1$	
$\{c_n^{(0)}\}_i$	$a_i^{(0)} \times \{a_n^{(0)}\}$	$a_i^{(0)} \times (a_0^{(0)}, a_1^{(0)}, a_2^{(0)}, \dots, a_{w-1}^{(0)})$
$\{c_n^{(1)}\}_i$	$a_i^{(1)} \times \{a_n^{(1)}\}$	$a_i^{(1)} \times (a_0^{(1)}, a_1^{(1)}, a_2^{(1)}, \dots, a_{w-1}^{(1)})$
$\{c_n^{(2)}\}_i$	$a_i^{(2)} \times \{a_n^{(2)}\}$	$a_i^{(2)} \times (a_0^{(2)}, a_1^{(2)}, a_2^{(2)}, \dots, a_{w-1}^{(2)})$
...	...	...
$\{c_n^{(m-1)}\}_i$	$a_i^{(m-1)} \times \{a_n^{(m-1)}\}$	$a_i^{(m-1)} \times (a_0^{(m-1)}, a_1^{(m-1)}, a_2^{(m-1)}, \dots, a_{w-1}^{(m-1)})$

The  $i$ -th subset of sequences, denoted by  $\{b^{(q)}\}_i$ , is constructed by concatenating the sequences of the  $i$ -th coset,  $\{c^{(m)}\}_i$ , according to a predefined order, where a subset contains  $q$  sequences  $\{b_k^{(i)}\}$  each of length  $N = q \times w$ . The order by which sequences of a coset are concatenated is determined by an Addition table constructed on the powers of a primitive root or primitive element using modular arithmetic and a finite set of integers or polynomials determined by the value of  $m$ . The construction of Addition tables is illustrated by way of example below. Finally, a set of Structured Codes, denoted by  $\{s^{(N)}\}$ , is constructed by sequentially concatenating the  $w$  subsets  $\{b^{(q)}\}_i$  for  $0 \leq i \leq w-1$ . A set of Structured Codes contains  $N$  sequences each of length  $N = q \times w$ . Structured Codes are constructed for three conditions depending on  $m$ .

10

15

### **Condition 1: "m = odd prime integer"**

The procedure for constructing a set of Structured Codes is illustrated by way of example when  $m = 5$ . Firstly, a seed set  $\{a^{(5)}\}$  is selected as illustrated below.

20

$\{a^{(5)}\}$	Seed Set
$\{a_n^{(0)}\}$	++++-
$\{a_n^{(1)}\}$	+++--
$\{a_n^{(2)}\}$	++-++
$\{a_n^{(3)}\}$	+--++
$\{a_n^{(4)}\}$	-++++



In this example, each sequence in the seed set has length  $w = 5$ . We construct  $w = 5$  cosets using the procedure described above for  $i = 0, 1, 2, 3$  and  $4$  as illustrated below.

$Z_m$	$\{c^{(5)}\}_i$	$\{c^{(5)}\}_0$	$\{c^{(5)}\}_1$	$\{c^{(5)}\}_2$	$\{c^{(5)}\}_3$	$\{c^{(5)}\}_4$
0	$\{c_n^{(0)}\}_i$	++++-	++++-	++++-	++++-	-----
1	$\{c_n^{(1)}\}_i$	+++--	+++--	+++--	-----	+++++
2	$\{c_n^{(2)}\}_i$	++-++	++-++	--++-	++-++	+++++
3	$\{c_n^{(3)}\}_i$	+-----	+-----	+-----	+-----	+-----
4	$\{c_n^{(4)}\}_i$	+-----	+-----	+-----	+-----	+-----

- 5 When  $m$  is an odd prime, the integer residue class  $Z_m = \{0, 1, 2, \dots, m-1\}$  form a Galois field,  $GF(m)$ , with respect to addition and multiplication modulo  $m$ . If  $a$  is a primitive root of  $m$  then there are  $\phi(m) = m-1$  residue integers  $Z_l$  relatively prime to  $m$ , (i.e.  $\gcd(l, m) = 1$ ), which can be used to construct an Addition table  $A(q)$ , where  $q = \phi(m)+1$  and  $\phi(\cdot)$  is the Euler totient function. When  $a$  is a primitive root of  $m$  then the powers of  $a$ , namely  $a^0, a^1, a^2, \dots, a^{m-2}$ , are all distinct modulo  $m$  and correspond to the non-zero residue integers  $Z_l$ . That is, each residue integer  $Z_l$  can be expressed as a power of the primitive root  $a$ . Correspondingly, an Addition table over  $GF(m)$  based on the powers of  $a$  modulo  $m$  can be constructed. Thus,  $a = 2$  is a primitive root of  $m = 5$  and the powers of  $a$  modulo  $m$  are  $(a^0, a^1, a^2, a^3) = (1, 2, 4, 3)$ . Hence,  $q = \phi(5)+1 = 5$  and the corresponding Addition table  $A(5)$  is illustrated below.

+		0	$a^0$	$a^1$	$a^2$	$a^3$
		0	1	2	4	3
0	0	0	1	2	4	3
$a^0$	1	1	2	3	0	4
$a^1$	2	2	3	4	1	0
$a^2$	4	4	0	1	3	2
$a^3$	3	3	4	0	2	1

Addition table-1 over  $GF(5)$  for  $a = 2$

- 20 We construct a subset  $\{b^{(q)}\}_i$  corresponding to each coset  $\{c^{(m)}\}_i$  by concatenating the sequences of  $\{c^{(m)}\}_i$  according to the rows of the Addition table  $A(5)$  as illustrated below.

$\{b^{(5)}\}_i$	$i$ -th Subset for $0 \leq i \leq w-1$
$\{b_k^{(0)}\}_i$	$\{c_n^{(0)}\}_i \{c_n^{(1)}\}_i \{c_n^{(2)}\}_i \{c_n^{(4)}\}_i \{c_n^{(3)}\}_i$
$\{b_k^{(1)}\}_i$	$\{c_n^{(1)}\}_i \{c_n^{(2)}\}_i \{c_n^{(3)}\}_i \{c_n^{(0)}\}_i \{c_n^{(4)}\}_i$
$\{b_k^{(2)}\}_i$	$\{c_n^{(2)}\}_i \{c_n^{(3)}\}_i \{c_n^{(4)}\}_i \{c_n^{(1)}\}_i \{c_n^{(0)}\}_i$
$\{b_k^{(3)}\}_i$	$\{c_n^{(4)}\}_i \{c_n^{(0)}\}_i \{c_n^{(1)}\}_i \{c_n^{(3)}\}_i \{c_n^{(2)}\}_i$
$\{b_k^{(4)}\}_i$	$\{c_n^{(3)}\}_i \{c_n^{(4)}\}_i \{c_n^{(0)}\}_i \{c_n^{(2)}\}_i \{c_n^{(1)}\}_i$

The subsets  $\{b^{(5)}\}_i$  for  $i = 0, 1, 2, 3$  and  $4$  are illustrated below.

$\{b^{(5)}\}_0$	Subset 0
$\{b_k^{(0)}\}_0$	++++- +++++ +---+ +----- +-----
$\{b_k^{(1)}\}_0$	++++- +++++ +---+ +----- +-----
$\{b_k^{(2)}\}_0$	++++- +++++ +---+ +----- +-----
$\{b_k^{(3)}\}_0$	++++- +++++ +---+ +----- +-----
$\{b_k^{(4)}\}_0$	++++- +++++ +---+ +----- +-----
$\{b^{(5)}\}_1$	Subset 1
$\{b_k^{(0)}\}_1$	++++- +++++ +---+ +----- +-----
$\{b_k^{(1)}\}_1$	++++- +++++ +---+ +----- +-----
$\{b_k^{(2)}\}_1$	++++- +++++ +---+ +----- +-----
$\{b_k^{(3)}\}_1$	++++- +++++ +---+ +----- +-----
$\{b_k^{(4)}\}_1$	++++- +++++ +---+ +----- +-----
$\{b^{(5)}\}_2$	Subset 2
$\{b_k^{(0)}\}_2$	++++- +++++ +---+ +----- +-----
$\{b_k^{(1)}\}_2$	++++- +++++ +---+ +----- +-----
$\{b_k^{(2)}\}_2$	++++- +++++ +---+ +----- +-----
$\{b_k^{(3)}\}_2$	++++- +++++ +---+ +----- +-----
$\{b_k^{(4)}\}_2$	++++- +++++ +---+ +----- +-----
$\{b^{(5)}\}_3$	Subset 3
$\{b_k^{(0)}\}_3$	++++- +++++ +---+ +----- +-----
$\{b_k^{(1)}\}_3$	++++- +++++ +---+ +----- +-----
$\{b_k^{(2)}\}_3$	++++- +++++ +---+ +----- +-----
$\{b_k^{(3)}\}_3$	++++- +++++ +---+ +----- +-----
$\{b_k^{(4)}\}_3$	++++- +++++ +---+ +----- +-----
$\{b^{(5)}\}_4$	Subset 4
$\{b_k^{(0)}\}_4$	++++- +++++ +---+ +----- +-----
$\{b_k^{(1)}\}_4$	++++- +++++ +---+ +----- +-----
$\{b_k^{(2)}\}_4$	++++- +++++ +---+ +----- +-----
$\{b_k^{(3)}\}_4$	++++- +++++ +---+ +----- +-----
$\{b_k^{(4)}\}_0$	++++- +++++ +---+ +----- +-----

- 5 Finally, a set of Structured Codes  $\{s^{(N)}\}$ , which contains  $N$  outer sequences,  $\{s_k^{(i)}\}$ , each of length  $N$  where  $N = q \times w = 25$ , is constructed by sequentially concatenating the subsets  $\{b^{(5)}\}_i$  for  $i = 0, 1, 2, 3$  and  $4$  as illustrated below.

$\{s^{(25)}\}$	Set of Structured Codes
$\{s_k^{(0)}\}$	++++-+++-----+---
$\{s_k^{(1)}\}$	+++-----+-----+---
$\{s_k^{(2)}\}$	+++-----+-----+---
$\{s_k^{(3)}\}$	+-----+-----+-----+---
$\{s_k^{(4)}\}$	+-----+-----+-----+---
$\{s_k^{(5)}\}$	+++++-----+-----+---
$\{s_k^{(6)}\}$	+++++-----+-----+---
$\{s_k^{(7)}\}$	++-+-+-----+-----+---
$\{s_k^{(8)}\}$	-+++++-----+-----+---
$\{s_k^{(9)}\}$	+-+-----+-----+-----+---
$\{s_k^{(10)}\}$	+++++-----+-----+---
$\{s_k^{(11)}\}$	+++--+-----+-----+---
$\{s_k^{(12)}\}$	--+-----+-----+-----+---
$\{s_k^{(13)}\}$	-+++++-----+-----+---
$\{s_k^{(14)}\}$	+-----+-----+-----+---
$\{s_k^{(15)}\}$	+++++-----+-----+---
$\{s_k^{(16)}\}$	-----+-----+-----+---
$\{s_k^{(17)}\}$	++-+-+-----+-----+---
$\{s_k^{(18)}\}$	-+++++-----+-----+---
$\{s_k^{(19)}\}$	+-----+-----+-----+---
$\{s_k^{(20)}\}$	-----+-----+-----+---
$\{s_k^{(21)}\}$	+++++-----+-----+---
$\{s_k^{(22)}\}$	++-+-+-----+-----+---
$\{s_k^{(23)}\}$	-+++++-----+-----+---
$\{s_k^{(24)}\}$	+-----+-----+-----+---

For the primitive root  $a = 2$  we can construct another three distinct Addition tables over  $GF(5)$ . Firstly, the Multiplication table over  $GF(5)$  based on the powers of  $a$  modulo  $m$  is constructed. Secondly, each non-zero row of the Multiplication table is used to construct a distinct Addition table. The first non-zero row of the Multiplication table constructs Addition table-1 used above while the following three non-zero rows construct another three distinct Addition tables as illustrated below.

X		0	$a^0$	$a^1$	$a^2$	$a^3$
		0	1	2	4	3
0	0	0	0	0	0	0
$a^0$	1	0	1	2	4	3
$a^1$	2	0	2	4	3	1
$a^2$	4	0	4	3	1	2
$a^3$	3	0	3	1	2	4

Multiplication table-1 over GF(5) for  $a = 2$

- 18 -

+	0	2	4	3	1
0	0	2	4	3	1
2	2	4	1	0	3
4	4	1	3	2	0
3	3	0	2	1	4
1	1	3	0	4	2

Addition table-2 over GF(5) for  $a = 2$ 

+	0	4	3	1	2
0	0	4	3	1	2
4	4	3	2	0	1
3	3	2	1	4	0
1	1	0	4	2	3
2	2	1	0	3	4

Addition table-3 over GF(5) for  $a = 2$ 

+	0	3	1	2	4
0	0	3	1	2	4
3	3	1	4	0	2
1	1	4	2	3	0
2	2	0	3	4	1
4	4	2	0	1	3

Addition table-4 over GF(5) for  $a = 2$ 

5

Each Addition table can be used to construct a distinct set of Structured Codes from the same seed set by uniquely specifying the concatenation order of coset sequences within a subset. Since for primitive root  $a = 2$  there are four distinct Addition tables then we can construct four distinct sets of Structured Codes for the seed set specified.

10

Furthermore, the integer  $m = 5$  has two primitive roots,  $a = 2$  and  $a = 3$ . In this case a second distinct Multiplication table over GF(5) based on the powers of  $a = 3$  modulo  $m$  can be constructed as illustrated below.

15

- 19 -

$\times$		0	$a^0$	$a^1$	$a^2$	$a^3$
		0	1	3	4	2
0	0	0	0	0	0	0
$a^0$	1	0	1	3	4	2
$a^1$	3	0	3	4	2	1
$a^2$	4	0	4	2	1	3
$a^3$	2	0	2	1	3	4

Multiplication table-2 over GF(5) for  $a = 3$ 

As before, each non zero row of the Multiplication table over GF(5) for  $a = 3$  can be used to construct four distinct Addition tables which in turn can be used to construct four  
 5 distinct sets of Structured Codes from the same seed set. Hence, when  $m = 5$  it is possible to construct a total of eight distinct sets of Structured Codes from one seed set.

Since the number of available seed sets is large and since the number of available Addition  
 10 tables is large, then the number and variety of sets of Structured Codes is very large indeed. Therefore, the large code space covered by the Structured Codes make their application to spread spectrum communication systems ideal.

In summary, when  $m$  is an odd prime number sets of Structured Codes are constructed by selecting a seed set, constructing cosets, constructing subsets using Addition tables derived  
 15 from Multiplication tables over GF( $m$ ) that specify the unique concatenation order of inner sequences and finally sequentially concatenating subsets to form a full set of Structured Codes.

**Condition 2: " $m = \text{non-prime integer}$ "**

20 The procedure for constructing a set of Structured Codes when  $m$  is non-prime is illustrated by way of example for  $m = 10$ . Firstly, a seed set  $\{a^{(10)}\}$  is selected as illustrated below.

- 20 -

$\{a^{(10)}\}$	Seed Set
$\{a_n^{(0)}\}$	+++++++--
$\{a_n^{(1)}\}$	+++++++--+
$\{a_n^{(2)}\}$	+++++++--+
$\{a_n^{(3)}\}$	+++++++--++
$\{a_n^{(4)}\}$	+++++--++++
$\{a_n^{(5)}\}$	++++-+++++
$\{a_n^{(6)}\}$	+++-+++++
$\{a_n^{(7)}\}$	++-+++++
$\{a_n^{(8)}\}$	+---+++++
$\{a_n^{(9)}\}$	-+++++

In this example, each sequence in the seed set has length  $w = 10$ . We construct  $w = 10$  cosets for  $0 \leq i \leq 9$  as illustrated below.

$Z_m$	$\{c^{(10)}\}_i$	$\{c^{(10)}\}_0$	$\{c^{(10)}\}_1$	$\{c^{(10)}\}_2$	$\{c^{(10)}\}_3$	$\{c^{(10)}\}_4$
0	$\{c_n^{(0)}\}_i$	+++++++--	+++++++--	+++++++--	+++++++--	+++++++--
1	$\{c_n^{(1)}\}_i$	+++++++--+	+++++++--+	+++++++--+	+++++++--+	+++++++--+
2	$\{c_n^{(2)}\}_i$	+++++++--+	+++++++--+	+++++++--+	+++++++--+	+++++++--+
3	$\{c_n^{(3)}\}_i$	+++++++--++	+++++++--++	+++++++--++	+++++++--++	+++++++--++
4	$\{c_n^{(4)}\}_i$	+++++--++++	+++++--++++	+++++--++++	+++++--++++	+++++--++++
5	$\{c_n^{(5)}\}_i$	++++-+++++	++++-+++++	++++-+++++	++++-+++++	++++-+++++
6	$\{c_n^{(6)}\}_i$	+++-+++++	+++-+++++	+++-+++++	+++-+++++	+++-+++++
7	$\{c_n^{(7)}\}_i$	++-+++++	++-+++++	++-+++++	++-+++++	++-+++++
8	$\{c_n^{(8)}\}_i$	+---+++++	+---+++++	+---+++++	+---+++++	+---+++++
9	$\{c_n^{(9)}\}_i$	-+++++	-+++++	-+++++	-+++++	-+++++

5

$Z_m$	$\{c^{(10)}\}_i$	$\{c^{(10)}\}_5$	$\{c^{(10)}\}_6$	$\{c^{(10)}\}_7$	$\{c^{(10)}\}_8$	$\{c^{(10)}\}_9$
0	$\{c_n^{(0)}\}_i$	+++++++--	+++++++--	+++++++--	+++++++--	-----+
1	$\{c_n^{(1)}\}_i$	+++++++--+	+++++++--+	+++++++--+	-----+	+++++++--+
2	$\{c_n^{(2)}\}_i$	+++++++--+	+++++++--+	+++++++--+	+++++++--+	+++++++--+
3	$\{c_n^{(3)}\}_i$	+++++++--++	+++++++--++	+++++++--++	+++++++--++	+++++++--++
4	$\{c_n^{(4)}\}_i$	+++++--++++	+++++--++++	+++++--++++	+++++--++++	+++++--++++
5	$\{c_n^{(5)}\}_i$	++++-+++++	++++-+++++	++++-+++++	++++-+++++	++++-+++++
6	$\{c_n^{(6)}\}_i$	+++-+++++	+++-+++++	+++-+++++	+++-+++++	+++-+++++
7	$\{c_n^{(7)}\}_i$	++-+++++	++-+++++	++-+++++	++-+++++	++-+++++
8	$\{c_n^{(8)}\}_i$	+---+++++	+---+++++	+---+++++	+---+++++	+---+++++
9	$\{c_n^{(9)}\}_i$	-+++++	-+++++	-+++++	-+++++	-+++++

- When  $m$  is non-prime, the integer residue class  $Z_m = \{0, 1, 2, \dots, m-1\}$  form a finite Ring,  $R(m)$ , with respect to addition and multiplication modulo  $m$ . If  $a$  is a primitive root of  $m$  then there are  $\phi(m)$  residue integers  $Z_l$  relatively prime to  $m$ , (i.e.  $\gcd(l, m) = 1$ ), which can be used to construct an Addition table  $A(q)$ , where  $q = \phi(m)+1$  and  $\phi(\cdot)$  is the Euler totient function. When  $a$  is a primitive root of  $m$  then the powers of  $a$ , namely  $a^0, a^1, a^2, \dots, a^{\phi(m)-1}$ ,

- 21 -

are all distinct modulo  $m$  and correspond to the non-zero residue integers  $Z_i$ . That is, each residue integer  $Z_i$  can be expressed as a power of the primitive root  $a$ . Correspondingly, an Addition table over  $R(m)$  based on the powers of  $a$  modulo  $m$  can be constructed. Thus,  $a = 3$  is a primitive root of  $m = 10$  and the powers of  $a$  modulo  $m$  are  $(a^0, a^1, a^2, a^3) = (1, 3, 9, 7)$ . Hence,  $q = \phi(10)+1 = 5$  and the corresponding Addition table A(5) is illustrated below.

+		0	$a^0$	$a^1$	$a^2$	$a^3$
		0	1	3	9	7
0	0	0	1	3	9	7
$a^0$	1	1	2	4	0	8
$a^1$	3	3	4	6	2	0
$a^2$	9	9	0	2	8	6
$a^3$	7	7	8	0	6	4

Addition table-1 over  $R(10)$  for  $a = 3$ 

We construct a subset  $\{b^{(q)}\}_i$  corresponding to each coset  $\{c^{(m)}\}_i$  by concatenating the sequences of  $\{c^{(m)}\}_i$  according to the rows of the Addition table A(5) as illustrated below.

$\{b^{(5)}\}_i$	$i$ -th Subset for $0 \leq i \leq w-1$
$\{b_k^{(0)}\}_i$	$\{c_n^{(0)}\}_i \{c_n^{(1)}\}_i \{c_n^{(3)}\}_i \{c_n^{(9)}\}_i \{c_n^{(7)}\}_i$
$\{b_k^{(1)}\}_i$	$\{c_n^{(1)}\}_i \{c_n^{(2)}\}_i \{c_n^{(4)}\}_i \{c_n^{(0)}\}_i \{c_n^{(8)}\}_i$
$\{b_k^{(2)}\}_i$	$\{c_n^{(3)}\}_i \{c_n^{(4)}\}_i \{c_n^{(6)}\}_i \{c_n^{(2)}\}_i \{c_n^{(0)}\}_i$
$\{b_k^{(3)}\}_i$	$\{c_n^{(9)}\}_i \{c_n^{(0)}\}_i \{c_n^{(2)}\}_i \{c_n^{(8)}\}_i \{c_n^{(6)}\}_i$
$\{b_k^{(4)}\}_i$	$\{c_n^{(7)}\}_i \{c_n^{(8)}\}_i \{c_n^{(0)}\}_i \{c_n^{(6)}\}_i \{c_n^{(4)}\}_i$

Finally, a set of Structured Codes  $\{s^{(M)}\}$ , which contains  $N$  outer sequences,  $\{s_k^{(\cdot)}\}$ , each of length  $N$ , where  $N = q \times w = 50$ , is constructed by sequentially concatenating the subsets  $\{b^{(5)}\}_i$  for  $i = 0, 1, 2, 3, 4, 5, 6, 7, 8$  and  $9$  as illustrated below.

$\{S^{(50)}\}$	Set of Structured Codes
$\{S_k^{(0)}\}$	+++++++-----+-----+++++
$\{S_k^{(1)}\}$	+++++++-----+-----+++++
$\{S_k^{(2)}\}$	+++++++-----+-----+++++
$\{S_k^{(3)}\}$	+++++++-----+-----+++++
$\{S_k^{(4)}\}$	+++++++-----+-----+++++
$\{S_k^{(5)}\}$	+++++++-----+-----+++++
$\{S_k^{(6)}\}$	+++++++-----+-----+++++
$\{S_k^{(7)}\}$	+++++++-----+-----+++++
$\{S_k^{(8)}\}$	+++++++-----+-----+++++
$\{S_k^{(9)}\}$	+++++++-----+-----+++++
$\{S_k^{(10)}\}$	+++++++-----+-----+++++
$\{S_k^{(11)}\}$	+++++++-----+-----+++++
$\{S_k^{(12)}\}$	+++++++-----+-----+++++
$\{S_k^{(13)}\}$	+++++++-----+-----+++++
$\{S_k^{(14)}\}$	+++++++-----+-----+++++
$\{S_k^{(15)}\}$	+++++++-----+-----+++++
$\{S_k^{(16)}\}$	+++++++-----+-----+++++
$\{S_k^{(17)}\}$	+++++++-----+-----+++++
$\{S_k^{(18)}\}$	+++++++-----+-----+++++
$\{S_k^{(19)}\}$	+++++++-----+-----+++++
$\{S_k^{(20)}\}$	+++++++-----+-----+++++
$\{S_k^{(21)}\}$	+++++++-----+-----+++++
$\{S_k^{(22)}\}$	+++++++-----+-----+++++
$\{S_k^{(23)}\}$	+++++++-----+-----+++++
$\{S_k^{(24)}\}$	+++++++-----+-----+++++
$\{S_k^{(25)}\}$	+++++++-----+-----+++++
$\{S_k^{(26)}\}$	+++++++-----+-----+++++
$\{S_k^{(27)}\}$	+++++++-----+-----+++++
$\{S_k^{(28)}\}$	+++++++-----+-----+++++
$\{S_k^{(29)}\}$	+++++++-----+-----+++++
$\{S_k^{(30)}\}$	+++++++-----+-----+++++
$\{S_k^{(31)}\}$	+++++++-----+-----+++++
$\{S_k^{(32)}\}$	+++++++-----+-----+++++
$\{S_k^{(33)}\}$	+++++++-----+-----+++++
$\{S_k^{(34)}\}$	+++++++-----+-----+++++
$\{S_k^{(35)}\}$	+++++++-----+-----+++++
$\{S_k^{(36)}\}$	+++++++-----+-----+++++
$\{S_k^{(37)}\}$	+++++++-----+-----+++++
$\{S_k^{(38)}\}$	+++++++-----+-----+++++
$\{S_k^{(39)}\}$	+++++++-----+-----+++++
$\{S_k^{(40)}\}$	+++++++-----+-----+++++
$\{S_k^{(41)}\}$	+++++++-----+-----+++++
$\{S_k^{(42)}\}$	+++++++-----+-----+++++
$\{S_k^{(43)}\}$	+++++++-----+-----+++++
$\{S_k^{(44)}\}$	+++++++-----+-----+++++
$\{S_k^{(45)}\}$	+++++++-----+-----+++++
$\{S_k^{(46)}\}$	+++++++-----+-----+++++
$\{S_k^{(47)}\}$	+++++++-----+-----+++++
$\{S_k^{(48)}\}$	+++++++-----+-----+++++
$\{S_k^{(49)}\}$	+++++++-----+-----+++++



- For the primitive root  $a = 3$  we can construct another three distinct Addition tables over  $R(10)$ . Firstly, the Multiplication table over  $R(10)$  based on the powers of  $a$  modulo  $m$  is constructed. Secondly, each non-zero row of the Multiplication table is used to construct a distinct Addition table. The first non-zero row of the Multiplication table constructs
- 5 Addition table-1 over  $R(10)$  used above while the following three non-zero rows construct another three distinct Addition tables over  $R(10)$  as illustrated below.

$\times$		0	$a^0$	$a^1$	$a^2$	$a^3$
		0	1	3	9	7
0	0	0	0	0	0	0
$a^0$	1	0	1	3	9	7
$a^1$	3	0	3	9	7	1
$a^2$	9	0	9	7	1	3
$a^3$	7	0	7	1	3	9

Multiplication table-1 over  $R(10)$  for  $a = 3$ 

+	0	3	9	7	1
0	0	3	9	7	1
3	3	6	2	0	4
9	9	2	8	6	0
7	7	0	6	4	8
1	1	4	0	8	2

Addition table-2 over  $R(10)$  for  $a = 3$ 

+	0	9	7	1	3
0	0	9	7	1	3
9	9	8	6	0	2
7	7	6	4	8	0
1	1	0	8	2	4
3	3	2	0	4	6

Addition table-3 over  $R(10)$  for  $a = 3$

- 24 -

+	0	7	1	3	9
0	0	7	1	3	9
7	7	4	8	0	6
1	1	8	2	4	0
3	3	0	4	6	2
9	9	6	0	2	8

Addition table-4 over  $R(10)$  for  $a = 3$ 

Each Addition table can be used to construct a set of Structured Codes from the same seed set by uniquely specifying the concatenation order of coset sequences within a subset.

Since for primitive root  $a = 3$  there are four distinct Addition tables then we can construct four sets of Structured Codes for the seed set specified.

Furthermore, the non-prime integer  $m = 10$  has two primitive roots,  $a = 3$  and  $a = 7$ . In this case a second distinct Multiplication table over  $R(10)$  based on the powers of  $a = 7$  modulo  $m$  can be constructed as illustrated below.

$\times$		0	$a^0$	$a^1$	$a^2$	$a^3$
		0	1	7	9	3
0	0	0	0	0	0	0
$a^0$	1	0	1	7	9	3
$a^1$	7	0	7	9	3	1
$a^2$	9	0	9	3	1	7
$a^3$	3	0	3	1	7	9

Multiplication table-2 over  $R(10)$  for  $a = 7$ 

As before, each non zero row of the Multiplication table over  $R(10)$  for  $a = 7$  can be used to construct four distinct Addition tables which in turn can be used to construct four sets of Structured Codes from the same seed set. Hence, when  $m = 10$  it is possible to construct a total of eight sets of Structured Codes from one seed set.

In general, when  $m$  is non-prime, the sets of Structured Codes constructed have inferior properties compared to those constructed when  $m$  is an odd prime integer.

In summary, when  $m$  is a non-prime number sets of Structured Codes are constructed by selecting a seed set, constructing cosets, constructing subsets using Addition tables derived from Multiplication tables over  $R(m)$  that specify the unique concatenation order of inner sequences and finally sequentially concatenating subsets to form a full set of Structured Codes.

**Condition 3: " $m = p^s$  when  $p$  is prime"**

A Galois field can be constructed for any prime number  $p$  or any integer power of a prime number  $p^s$ . The Galois field  $GF(p^s)$  having  $p^s$  elements is called an extension field of the Galois field  $GF(p)$  having  $p$  elements. The elements of  $GF(p)$  are the integer residue class  $Z_p = \{0, 1, 2, \dots, p-1\}$  with field addition and multiplication being carried out modulo  $p$ . The elements of  $GF(p^s)$  are polynomials of degree  $\leq s-1$  over  $GF(p)$ , i.e. the coefficients of the polynomials are elements in  $GF(p)$ . Then field addition and multiplication are carried out modulo  $g(x)$  where  $g(x)$  is a primitive polynomial of degree  $s$  over  $GF(p)$ . A polynomial of degree  $s$  is said to be primitive if the smallest integer  $r$  for which  $g(x)$  divides  $x^r + 1$  is  $p^s - 1$ . Primitive polynomials are irreducible because they can not be factorised (i.e. they are not the product of any two polynomials of lower degree).

The procedure for constructing a set of Structured Codes is illustrated by way of example when  $m = 2^2$ , that is,  $p = 2$  and  $s = 2$ . Firstly, a seed set  $\{a^{(4)}\}$  is selected as illustrated below.

$\{a^{(4)}\}$	Seed Set
$\{a_n^{(0)}\}$	+++-
$\{a_n^{(1)}\}$	+- -+
$\{a_n^{(2)}\}$	+ - ++
$\{a_n^{(3)}\}$	- +++

In this example, each sequence in the seed set has length  $w = 4$ . We construct  $w = 4$  cosets using the procedure described above for  $i = 0, 1, 2$ , and  $3$  as illustrated below.

$Z_m$	$Z_p[x]$	$\{c^{(4)}\}_i$	$\{c^{(4)}\}_0$	$\{c^{(4)}\}_1$	$\{c^{(4)}\}_2$	$\{c^{(4)}\}_3$
0	0	$\{c_n^{(0)}\}_i$	+++ -	+++ -	+++ -	--- +
1	1	$\{c_n^{(1)}\}_i$	+++ +	+++ +	--- -	+++ +
2	$x$	$\{c_n^{(2)}\}_i$	+++ +	-+ - -	+ - + +	+ - + +
3	$x+1$	$\{c_n^{(3)}\}_i$	+ - - -	- + + +	- + + +	- + + +

- Let  $Z_p[x]$  denote the residue classes of polynomials modulo  $g(x)$  in the variable  $x$ . Then  $Z_p[x]$  is the set of polynomials modulo  $g(x)$  each with degree less than the degree of  $g(x)$ .
- 5 When  $g(x)$  is a primitive polynomial of degree  $s$  over  $GF(p)$ , then  $Z_p[x]$  forms a Galois polynomial field  $GF(p^s)$  with respect to addition and multiplication modulo  $g(x)$ . The Galois field  $GF(p^s)$  contains  $p^s$  elements corresponding to the residue classes of polynomials  $g(x)$ . If  $\alpha$  is a primitive element of  $GF(p^s)$ , where there are exactly  $\phi(p^s-1)$  primitive elements, then the powers of  $\alpha$ , namely  $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{p^s-2}$ , are all distinct
- 10 modulo  $g(x)$  and correspond to the non-zero residue polynomials in  $Z_p[x]$ . That is, each residue polynomial can be expressed as a power of the primitive element  $\alpha$ .
- Correspondingly, an Addition table over  $GF(p^s)$  based on the powers of  $\alpha$  modulo  $g(x)$  can be constructed. Thus,  $\alpha = x$  is a primitive element of the primitive polynomial  $g(x) = x^2+x+1$  and the powers of  $\alpha$  modulo  $g(x)$  are  $(\alpha^0, \alpha^1, \alpha^2) = (1, x, x+1)$ . Hence,  $q = p^s = 2^2$
- 15 and the corresponding Addition table  $A(2^2)$  is illustrated below.

+		0	$\alpha^0$	$\alpha^1$	$\alpha^2$
		0	1	$x$	$x+1$
0	0	0	1	$x$	$x+1$
$\alpha^0$	1	1	0	$x+1$	$x$
$\alpha^1$	$x$	$x$	$x+1$	0	1
$\alpha^2$	$x+1$	$x+1$	$x$	1	0

Addition table-1 over  $GF(2^2)$  for  $\alpha = x$  and  $g(x) = x^2+x+1$

- We construct a subset  $\{b^{(q)}\}_i$  corresponding to each coset  $\{c^{(m)}\}_i$  by concatenating the sequences of  $\{c^{(m)}\}_i$  according to the rows of the Addition table  $A(2^2)$ . This procedure is
- 20 facilitated by assigning the integer residue class  $Z_{m=4} = \{0, 1, 2, 3\}$  to the polynomial residue class  $Z_{p=2}[x] = \{0, 1, x, x+1\}$  according to the sequential mapping  $0 \rightarrow 0, 1 \rightarrow 1, x \rightarrow 2$  and  $x+1 \rightarrow 3$ . Then the  $i$ -th subset  $\{b^{(4)}\}_i$  is illustrated below.

- 27 -

$\{b^{(4)}\}_i$	$i$ -th Subset for $0 \leq i \leq w-1$
$\{b_k^{(0)}\}_I$	$\{c_n^{(0)}\}_i \{c_n^{(1)}\}_i \{c_n^{(2)}\}_i \{c_n^{(3)}\}_i$
$\{b_k^{(1)}\}_I$	$\{c_n^{(1)}\}_i \{c_n^{(0)}\}_i \{c_n^{(3)}\}_i \{c_n^{(2)}\}_i$
$\{b_k^{(2)}\}_I$	$\{c_n^{(2)}\}_i \{c_n^{(3)}\}_i \{c_n^{(0)}\}_i \{c_n^{(1)}\}_i$
$\{b_k^{(3)}\}_I$	$\{c_n^{(3)}\}_i \{c_n^{(2)}\}_i \{c_n^{(1)}\}_i \{c_n^{(0)}\}_i$

The subsets  $\{b^{(4)}\}_i$  for  $i = 0, 1, 2$ , and 4 are illustrated below.

$\{b^{(4)}\}_0$	Subset 0
$\{b_k^{(0)}\}_0$	+++--++--++--++--
$\{b_k^{(1)}\}_0$	++-++++-++-++-
$\{b_k^{(2)}\}_0$	+---++-++-++-++-
$\{b_k^{(3)}\}_0$	+-++-++-++-++-
$\{b^{(4)}\}_1$	Subset 1
$\{b_k^{(0)}\}_1$	++++-++-++-++-
$\{b_k^{(1)}\}_1$	++-++++-++-++-
$\{b_k^{(2)}\}_1$	--++-++++-++-++-
$\{b_k^{(3)}\}_1$	---++-++-++-++-
$\{b^{(4)}\}_2$	Subset 2
$\{b_k^{(0)}\}_2$	++++-++-++-++-
$\{b_k^{(1)}\}_2$	--++-++++-++-++-
$\{b_k^{(2)}\}_2$	+---++-++-++-++-
$\{b_k^{(3)}\}_2$	---++-++-++-++-
$\{b^{(4)}\}_3$	Subset 3
$\{b_k^{(0)}\}_3$	---++-++-++-++-
$\{b_k^{(1)}\}_3$	++-++-++-++-++-
$\{b_k^{(2)}\}_3$	+---++-++-++-++-
$\{b_k^{(3)}\}_3$	---++-++-++-++-

- 5 Finally, a set of Structured Codes  $\{s^{(N)}\}$ , which contains  $N$  outer sequences,  $\{s_k^{(\cdot)}\}$ , each of length  $N$  where  $N = q \times w = 16$ , is constructed by sequentially concatenating the subsets  $\{b^{(4)}\}_i$  for  $i = 0, 1, 2$ , and 3 as illustrated below.

$\{S_k^{(16)}\}$	Structured Codes
$\{S_k^{(0)}\}$	+++--+--+--+--+---
$\{S_k^{(1)}\}$	++++++--+--+--+
$\{S_k^{(2)}\}$	+---+--+--+--+--+
$\{S_k^{(3)}\}$	+---+--+--+--+--+
$\{S_k^{(4)}\}$	++++++--+--+--+
$\{S_k^{(5)}\}$	++++++--+--+--+
$\{S_k^{(6)}\}$	-+---+--+--+--+
$\{S_k^{(7)}\}$	-+---+--+--+--+
$\{S_k^{(8)}\}$	++++++--+--+--+
$\{S_k^{(9)}\}$	-+---+--+--+--+
$\{S_k^{(10)}\}$	+---+--+--+--+--+
$\{S_k^{(11)}\}$	-+---+--+--+--+
$\{S_k^{(12)}\}$	-+---+--+--+--+
$\{S_k^{(13)}\}$	++++++--+--+--+
$\{S_k^{(14)}\}$	+---+--+--+--+--+
$\{S_k^{(15)}\}$	-+---+--+--+--+

For the primitive element  $\alpha = x$  we can construct another two distinct Addition tables over  $GF(2^2)$ . Firstly, the Multiplication table over  $GF(2^2)$  based on the powers of  $\alpha$  modulo  $g(x)$  is constructed. Secondly, each non-zero row of the Multiplication table is used to construct a distinct Addition table. The first non-zero row of the Multiplication table constructs Addition table-1 over  $GF(2^2)$  used above while the following two non-zero rows construct another two distinct Addition tables as illustrated below.

$\times$		0	$\alpha^0$	$\alpha^1$	$\alpha^2$
		0	1	x	x+1
0	0	0	0	0	0
$\alpha^0$	1	0	1	x	x+1
$\alpha^1$	x	0	x	x+1	1
$\alpha^2$	x+1	0	x+1	1	x

10

Multiplication table-1 over  $GF(2^2)$  for  $\alpha = x$  and  $g(x) = x^2+x+1$

+	0	x	x+1	1
0	0	x	x+1	1
x	x	0	1	x+1
x+1	x+1	1	0	x
1	1	x+1	x	0

Addition table-2 over  $GF(2^2)$  for  $\alpha = x$  and  $g(x) = x^2+x+1$

- 29 -

+	0	x+1	1	x
0	0	x+1	1	x
x+1	x+1	0	x	1
1	1	x	0	x+1
x	x	1	x+1	0

Addition table-3 over  $GF(2^2)$  for  $\alpha = x$  and  $g(x) = x^2 + x + 1$ 

Each Addition table can be used to construct a distinct set of Structured Codes from the same seed set by uniquely specifying the concatenation order of coset sequences within a subset. Since for primitive root  $\alpha = x$  there are three distinct Addition tables then we can construct three distinct sets of Structured Codes for the seed set specified.

Furthermore, the primitive polynomial  $g(x) = x^2 + x + 1$  has exactly  $\phi(p^s - 1) = \phi(2^2 - 1) = 2$  primitive elements,  $\alpha = x$  and  $\alpha = x+1$ . In this case a second distinct Multiplication table over  $GF(2^2)$  based on the powers of  $\alpha = x+1$  modulo  $g(x)$  can be constructed as illustrated below.

X		0	$\alpha^0$	$\alpha^1$	$\alpha^2$
		0	1	x+1	x
0	0	0	0	0	0
$\alpha^0$	1	0	1	x+1	x
$\alpha^1$	x+1	0	x+1	x	1
$\alpha^2$	x	0	x	1	x+1

Multiplication table-2 over  $GF(2^2)$  for  $\alpha = x+1$  and  $g(x) = x^2 + x + 1$ 

As before, each non zero row of the Multiplication table over  $GF(2^2)$  for  $\alpha = x+1$  can be used to construct three distinct Addition tables which in turn can be used to construct three distinct sets of Structured Codes from the same seed set.

Since there are exactly  $\phi(p^s - 1)$ 's distinct primitive polynomials of degree  $s$  in  $GF(p^s)$ , then there is only one primitive polynomial  $g(x) = x^2 + x + 1$  when  $m = 2^2$ . Hence, when  $m = 2^2$  it is possible to construct a total of six distinct sets of Structured Codes from one seed set.

- 30 -

In summary, when  $m = p^s$  where  $p$  is a prime number then sets of Structured Codes are constructed by selecting a seed set, constructing cosets, constructing subsets using Addition tables derived from Multiplication tables over  $GF(p^s)$  that specify the unique concatenation order of inner sequences and finally sequentially concatenating subsets to form a full set of Structured Codes.

### Alternative Constructs

When  $m$ , the number of sequences within a seed set, can not be characterised by one of the three conditions described above then an alternative construct can be used. In fact, this alternative construct may be used for any value of the integer  $m$ . However, the alternative construct is particularly useful when the integer  $m$  is non-prime and has no primitive roots. In this case, the  $\phi(m)$  residue integers  $Z_i$  relatively prime to  $m$  can not be generated from the powers of a primitive root because in this case the number  $m$  does not have any primitive roots. For the alternative construct, the integer residue class  $Z_m = \{0, 1, 2, \dots, m-1\}$  which form a finite ring  $R(m)$  is used directly to construct an Addition table modulo  $m$  over  $R(m)$ . For example, when  $m = 15$  the corresponding Addition table  $A(15)$  is illustrated below.

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	0	1	2	3	4	5	6	7	8	9	10	11	12	13



Addition table over  $R(15)$  using  $Z_{15}$ 

The  $i$ -th subset of sequences, denoted by  $\{b^{(q)}\}_i$ , is then constructed in the usual way by concatenating the sequences of the  $i$ -th coset,  $\{c^{(m)}\}_i$ , according to the predefined Addition table where  $q = m$  in this case. A set of Structured Codes, denoted by  $\{s^{(M)}\}$ , is constructed by sequentially concatenating the  $w$  subsets  $\{b^{(q)}\}_i$  for  $0 \leq i \leq w-1$ . The set of Structured Codes will contain  $N$  sequences each of length  $N = q \times w$ . For this construction rule only one Addition table can be constructed and therefore only one corresponding set of Structured Codes can be constructed.

10

A further refinement to the alternative construction rule is possible when  $m$  is non-prime and without primitive roots. Instead of using the integer residue class  $Z_m = \{0, 1, 2, \dots, m-1\}$  to construct an Addition table we can use the  $\phi(m)$  residue integers  $Z_l$  relatively prime to  $m$  to construct an Addition table. For example, when  $m = 15$ , the  $\phi(15) = 8$  residue integers relatively prime to 15 are  $\{1, 2, 4, 7, 8, 11, 13, 14\}$  and the corresponding Addition table is illustrated below.

15

+	0	1	2	4	7	8	11	13	14
0	0	1	2	4	7	8	11	13	14
1	1	2	3	5	8	9	12	14	0
2	2	3	4	6	9	10	13	0	1
4	4	5	6	8	11	12	0	2	3
7	7	8	9	11	14	0	3	5	6
8	8	9	10	12	0	1	4	6	7
11	11	12	13	0	3	4	7	9	10
13	13	14	0	2	5	6	9	11	12
14	14	0	1	3	6	7	10	12	13

Addition table-1 over  $R(15)$  using  $Z_l$  when  $m = 15$ 

20

Again, the  $i$ -th subset of sequences, denoted by  $\{b^{(q)}\}_i$ , is then constructed in the usual way by concatenating the sequences of the  $i$ -th coset,  $\{c^{(m)}\}_i$ , according to the predefined Addition table, where  $q = \phi(15)+1 = 9$  in this case. A set of Structured Codes, denoted by

$\{s^{(N)}\}$ , is constructed by sequentially concatenating the  $w$  subsets  $\{b^{(q)}\}_i$  for  $0 \leq i \leq w-1$ .

The set of Structured Codes will contains  $N$  sequences each of length  $N = q \times w$ .

Although  $m = 15$  has no primitive roots, we can construct another seven distinct Addition  
 5 tables over  $R(15)$ . Firstly, the Multiplication table over  $R(15)$  based on the  $\phi(15) = 8$   
 residue integers relatively prime to 15 is constructed as illustrated below.

$\times$	0	1	2	4	7	8	11	13	14
0	0	0	0	0	0	0	0	0	0
1	0	1	2	4	7	8	11	13	14
2	0	2	4	8	14	1	7	11	13
4	0	4	8	1	13	2	14	7	11
7	0	7	14	13	4	11	2	1	8
8	0	8	1	2	11	4	13	14	7
11	0	11	7	14	2	13	1	8	4
13	0	13	11	7	1	14	8	4	2
14	0	14	13	11	8	7	4	2	1

Multiplication table over  $R(15)$  using  $Z_l$  when  $m = 15$

10 Secondly, each non-zero row of the Multiplication table is used to construct a distinct  
 Addition table. The first non-zero row of the Multiplication table constructs Addition  
 table-1 over  $R(15)$  using  $Z_l$  when  $m = 15$  was illustrated above while the following seven  
 non-zero rows construct another seven distinct Addition tables over  $R(15)$  using  $Z_l$  when  $m$   
 = 15.

15

Each Addition table can be used to construct a set of Structured Codes from the same seed  
 set by uniquely specifying the concatenation order of coset sequences within a subset.  
 Since for  $m = 15$  there are eight distinct Addition tables over  $R(15)$  using  $Z_l$  when  $m = 15$   
 then we can construct eight sets of Structured Codes for a specified seed set. However,  
 20 because there are no primitive roots then only one Multiplication table can be constructed  
 in this case.

In a similar manner, a refinement to the alternative construction rule is possible when  $m = p^s$ . For any irreducible polynomial  $g(x)$  of degree  $s$  over  $GF(p)$  the residue classes  $Z_p[x]$  form a Galois polynomial field over  $GF(p)$  with respect to addition and multiplication modulo  $g(x)$ . The Galois polynomial field over  $GF(p)$  contains exactly  $p^s$  polynomial elements each of degree  $\leq s-1$  and each belonging to the residue classes of polynomials  $Z_p[x]$  modulo  $g(x)$ .

For this refinement, the only requirement is that the polynomial  $g(x)$  be irreducible. Then the residue classes  $Z_p[x]$  can be used directly to construct a distinct Multiplication table over  $GF(p^s)$ . However, only one multiplication table can be constructed for this case.

Subsequently, each non-zero row of the Multiplication table can be used to construct a distinct Addition table, which in turn defines the concatenation order of coset sequences that make up a subset. A further refinement in this case is also possible. When  $g(x)$  is a primitive polynomial then the construct described in Condition 3 is used since for any primitive element  $\alpha$  of  $GF(p^s)$  the powers of  $\alpha$ , namely  $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{p^s-2}$ , are all distinct modulo  $g(x)$  and correspond to the non-zero residue polynomials in  $Z_p[x]$ . That is, each residue polynomial can be expressed as a power of the primitive element  $\alpha$  and the order  $\varepsilon$  of the primitive element  $\alpha$  is equal to  $p^s-1$  such that  $\alpha^\varepsilon = 1$ . Correspondingly, Multiplication and an Addition tables over  $GF(p^s)$  based on all the powers of  $\alpha$  modulo  $g(x)$  can be constructed. However, if the polynomial  $g(x)$  is irreducible but not primitive then for any element  $\alpha$  of  $GF(p^s)$  the powers of  $\alpha$ , namely  $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{p^s-2}$ , are not all distinct modulo  $g(x)$ . Instead, if the order of element  $\alpha$  is  $\varepsilon$ , where  $\varepsilon < p^s-1$  but  $\varepsilon | p^s-1$  is the least positive integer for which  $\alpha^\varepsilon = 1$ , then the powers of  $\alpha$  up to  $\varepsilon-1$ , namely  $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{\varepsilon-1}$ , are distinct modulo  $g(x)$ . In this case it is possible to construct Multiplication and Addition tables over  $GF(p^s)$  based on the powers of  $\alpha$  up to  $\varepsilon-1$ , i.e.  $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{\varepsilon-1}$ , modulo  $g(x)$ . If this further refinement is used then it is preferable to choose an element  $\alpha$  with the largest possible value of  $\varepsilon$  where there are exactly  $\phi(\varepsilon)$  elements of order  $\varepsilon$  and hence it is possible to construct  $\phi(\varepsilon)$  Multiplication tables corresponding to the order  $\varepsilon$ . Once Addition tables are defined then the construction of Structured Codes can proceed as normal.

- 34 -

In summary, these refinements are included in order to complete the construction theory of Structured Codes. In practice, the most useful constructs are provided by Conditions 1, 3 and the Alternative Construct using the integer residue class  $Z_m$ . The constructs provided by Condition 2 and the refinements described above, when  $m$  is non-prime without  
 5 primitive roots or when  $g(x)$  is irreducible but not primitive, are less useful in practice but nonetheless complete.

The algorithms illustrated above provide a systematic way of constructing a very large number of sets of Structured Codes. In this section algorithms are illustrated that provide  
 10 guidelines for selecting seed sets that generate particularly useful Structured Codes for application in communication systems. Specifically, three families of Structured Codes are identified called Cyclical, Orthogonal and Balanced Structured Codes, respectively. The properties of a set of Structured Codes are underpinned by the seed set from which they are constructed. In general, a seed set can be selected from any family of sequences including  
 15 binary or non-binary, real or complex, quadriphase or polyphase etc. with corresponding mathematical operations being performed accordingly. For example, in the case of binary sequences there are  $2^w!/m!(2^w-m)!$  possible distinct seed sets consisting of  $m$  sequences each of length  $w$ . Hence, even for modest values of  $m$  and  $w$  the number of seed sets available is very large indeed. For example, when  $m=4$  and  $w=4$  there are 1820 available  
 20 binary seed sets.

In the case of binary sequences, a seed set could be constructed from any set of random binary sequences. However, the first and most obvious way to select a seed set is to choose it from a set of known sequences that have known good correlation properties. For  
 25 example, we can select the seed set from a set of  $m$ -sequences or Gold sequences or Gold-like sequences or small sets of Kasami sequences or large sets of Kasami sequences or Barker sequences or Legendre sequences or GMW sequences or Golay sequences or Frank sequences or Chu sequences or Huffman sequences etc. etc.. However, sets of Structured Codes with good correlation properties are obtained when the number  $m$  of sequences in  
 30 the seed set is equal to the length  $w$  of a seed sequence, that is,  $m=w$ . More specifically, if the binary sequence  $\{a_n\} = (a_0, a_1, a_2, \dots, a_{w-1})$  of length  $w$  is cyclically distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition

- 35 -

$$R(\tau) = \begin{cases} w & \text{for } \tau = 0 \\ \pm 1 & \text{for } \tau \neq 0 \end{cases}$$

then a seed set  $\{a^w\}$  constructed from the  $w$  left or right cyclical shifts of  $\{a_n\}$  produces  
 5 sets of Cyclical Structured Codes with good correlation properties. The term quasi-  
 balanced is taken to mean that the number of "+" and "-" elements in  $\{a_n\}$  differ by one.  
 The name Cyclical Structured Codes refers to the cyclical method used to construct the  
 seed set. Examples of sequences that are quasi-balanced and fulfill the optimal periodic  
 autocorrelation condition include all m-sequences, the binary Barker sequences (++-  
 10 ),(+++---+-) and (+++---+---+-), Legendre sequences when  $w = 4^{k-1}$  for integer  $k$  and  
 certain GMW sequences. Other binary sequences that fulfill these conditions do exist. The  
 procedure for constructing a seed set for generating a set of Cyclical Structured Codes is  
 illustrated by way of example below when  $m = w = 7$  and  $\{a_n\} = (+++---+-)$ , i.e. an m-  
 sequence.

15

$\{a^{(7)}\}$	Seed Set
$\{a_n^{(0)}\}$	+++---
$\{a_n^{(1)}\}$	++-+--
$\{a_n^{(2)}\}$	+--+--
$\{a_n^{(3)}\}$	-+--+--
$\{a_n^{(4)}\}$	---++--
$\{a_n^{(5)}\}$	----++
$\{a_n^{(6)}\}$	-----

One of the most significant constructs used in the generation of Structured Codes occurs  
 when the seed set is orthogonal and  $m = w$ . The term orthogonal is taken to mean that  
 every sequence in the seed set is orthogonal to every other sequence in the seed set. When  
 20 the seed set is orthogonal and  $m = w$  then the resulting set of Structured Codes is also  
 orthogonal. Sets of Structured Codes that are orthogonal have been called Orthogonal  
 Structured Codes. Hence, the identification of orthogonal seed sets is specifically relevant  
 to the generation of Orthogonal Structured Codes. It is almost certain that there is only one  
 periodic sequence that satisfies the ideal periodic autocorrelation condition shown below:

25

- 36 -

$$R(\tau) = \begin{cases} w & \text{for } \tau = 0 \\ 0 & \text{for } \tau \neq 0 \end{cases}$$

and this sequence is  $\{a_n\} = (+++-)$ . Then an orthogonal seed set  $\{a^{(4)}\}$  can be constructed from the four left or right cyclical shifts of  $\{a_n\}$  and the resulting set of Structured Codes  $\{s^{(16)}\}$  generated is also orthogonal. This particular example was demonstrated in Condition 3 earlier. A second systematic way of constructing Orthogonal Structured Codes is to use a Hadamard matrix as the seed set. A Hadamard matrix can be constructed for any integer power of 2 giving  $m = w = 2^s$ . Since the rows of an Hadamard matrix are always orthogonal then the Structured Codes generated are also orthogonal. A third systematic way of constructing Orthogonal Structured Codes is also based on the use of a binary sequence  $\{a_n\} = (a_0, a_1, a_2, \dots, a_{w-1})$  of length  $w$  that is cyclically distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition

$$R(\tau) = \begin{cases} w & \text{for } \tau = 0 \\ \pm 1 & \text{for } \tau \neq 0 \end{cases}$$

15

Firstly, a set of sequences is constructed from the  $w$  left or right cyclical shifts of  $\{a_n\}$ . Secondly, if  $R(\tau) = -1$  for  $\tau \neq 0$  then an additional sequence element equal to  $\{-1\}$  is appended to each sequence in the set and an additional sequence with all sequence elements equal to  $\{-1\}$  is appended to the set. Alternatively, if  $R(\tau) = +1$  for  $\tau \neq 0$  then an additional sequence element equal to  $\{+1\}$  is appended to each sequence in the set and an additional sequence with all sequence elements equal to  $\{+1\}$  is appended to the set. The resulting set of sequences thus form an orthogonal seed set. Examples of sequences that are quasi-balanced and fulfill the optimal periodic autocorrelation condition include all  $m$ -sequences, the binary Barker sequences  $(++-)$ ,  $(+++--+-)$  and  $(+++--+-+--)$ , Legendre sequences when  $w = 4^{k-1}$  for integer  $k$  and certain GMW sequences. Other binary sequences that fulfill these conditions do exist. The procedure for constructing an orthogonal seed set when  $\{a_n\}$  is cyclically distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition is illustrated by way of example below for  $\{a_n\} = (+++-+--)$ , i.e. an  $m$ -sequence.

30

$\{a^{(8)}\}$	Seed Set
$\{a_n^{(0)}\}$	+++----
$\{a_n^{(1)}\}$	++-+--+
$\{a_n^{(2)}\}$	+--+--+
$\{a_n^{(3)}\}$	-+--+--
$\{a_n^{(4)}\}$	+--+--+
$\{a_n^{(5)}\}$	--+++-+
$\{a_n^{(6)}\}$	-+++--+
$\{a_n^{(7)}\}$	-----

A fourth systematic way to construct a set of Orthogonal Structured Codes is to use a small set of Orthogonal Structured Codes as the seed set in the construction of a larger set of Orthogonal Structured Codes. A fifth systematic way to construct a set of Orthogonal Structured Codes is to select the seed set from a set of orthogonal Gold sequences.

One of the main constraints on a wireless communication system is the interference produced by co-channel effects, multiple access effects and multipath propagation effects. The effectiveness of spread spectrum techniques to combat the interference depends on the properties of the signature sequences used to spread the spectrum. The Structure Codes possess good autocorrelation and crosscorrelation properties for spread spectrum systems. The Orthogonal Structured Codes are of particular significance because each code is orthogonal to every other code in the set. Wireless communication networks based on spread spectrum techniques frequently use orthogonal sequences in order to cancel out the cross-interference between different sequences when correlated simultaneously in the same frequency band. Until now the set of orthogonal sequences most commonly used is the Walsh codes taken from the rows of a Hadamard matrix. However, only one set of Walsh codes exist per code length  $N$ , where  $N$  must be an integer power of two. The sequence construction algorithms described above extends the number of sets of Orthogonal Structured Codes per code length  $N$ . More importantly, the algorithms are capable of systematically constructing multiple sets of Orthogonal Structured Codes for most practical sequence lengths and beyond. In addition, a very useful property of Orthogonal Structured Codes is that they form a Complementary Set of sequences. That is, the aperiodic autocorrelation function of all sequences in a set of Orthogonal Structured Codes sum to zero for every time shift, except the zero shift.

- The flexibility of the construction rule for generating sets of Orthogonal Structured Codes is illustrated by way of example when  $m = 2^3$ , that is,  $p = 2$  and  $s = 3$ . Firstly, an orthogonal seed set  $\{a^{(8)}\}$  is constructed using the m-sequence  $\{a_n\} = (++++--)$  which is cyclically
- 5 distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition.

$\{a^{(8)}\}$	Seed Set
$\{a_n^{(0)}\}$	+++++---
$\{a_n^{(1)}\}$	++-+---+
$\{a_n^{(2)}\}$	+--+---+
$\{a_n^{(3)}\}$	-+---++-
$\{a_n^{(4)}\}$	+-+---++
$\{a_n^{(5)}\}$	--++---+
$\{a_n^{(6)}\}$	-+++---+
$\{a_n^{(7)}\}$	-----

In this example, each sequence in the seed set has length  $w = 8$ . We construct  $w = 8$  cosets using the procedure described above for  $i = 0, 1, 2, 3, 4, 5, 6$  and 7 as illustrated below.

10

$Z_m$	$Z_p[x]$	$\{c^{(8)}\}_1$	$\{c^{(8)}\}_0$	$\{c^{(8)}\}_1$	$\{c^{(8)}\}_2$	$\{c^{(8)}\}_3$
0	0	$\{c_n^{(0)}\}_i$	+++++---	+++++---	+++++---	-----++
1	1	$\{c_n^{(1)}\}_i$	++-+---+	++-+---+	---++---	++-+---+
2	$x$	$\{c_n^{(2)}\}_i$	+--+---+	-+---++-	+--+---+	-+---++-
3	$x+1$	$\{c_n^{(3)}\}_i$	-+---++-	-+---++-	-+---++-	-+---++-
4	$x^2$	$\{c_n^{(4)}\}_i$	+-+---++	+-+---++	+-+---++	+-+---++
5	$x^2+1$	$\{c_n^{(5)}\}_i$	+-+---++	+-+---++	+-+---++	+-+---++
6	$x^2+x$	$\{c_n^{(6)}\}_i$	+-+---++	+-+---++	+-+---++	+-+---++
7	$x^2+x+1$	$\{c_n^{(7)}\}_i$	+++++---	+++++---	+++++---	+++++---

$Z_m$	$Z_p[x]$	$\{c^{(8)}\}_1$	$\{c^{(8)}\}_4$	$\{c^{(8)}\}_5$	$\{c^{(8)}\}_6$	$\{c^{(8)}\}_7$
0	0	$\{c_n^{(0)}\}_i$	+++++---	---++---	---++---	---++---
1	1	$\{c_n^{(1)}\}_i$	---++---	---++---	---++---	---++---
2	$x$	$\{c_n^{(2)}\}_i$	---++---	---++---	---++---	---++---
3	$x+1$	$\{c_n^{(3)}\}_i$	---++---	---++---	---++---	---++---
4	$x^2$	$\{c_n^{(4)}\}_i$	---++---	---++---	---++---	---++---
5	$x^2+1$	$\{c_n^{(5)}\}_i$	---++---	---++---	---++---	---++---
6	$x^2+x$	$\{c_n^{(6)}\}_i$	---++---	---++---	---++---	---++---
7	$x^2+x+1$	$\{c_n^{(7)}\}_i$	+++++---	+++++---	+++++---	+++++---

- Since,  $\alpha = x$  is a primitive element of the primitive polynomial  $g(x) = x^3+x+1$  then the
- 15 powers of  $\alpha$  modulo  $g(x)$  are  $(\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6) = (1, x, x^2, x+1, x^2+x, x^2+x+1,$



- 39 -

$x^2+1$ ). Hence,  $q = p^s = 2^3$  and the corresponding Multiplication table  $M(2^3)$  over  $GF(2^3)$  modulo  $g(x) = x^3+x+1$  is illustrated below.

$\times$		0	$\alpha^0$	$\alpha^1$	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$
		0	1	x	$x^2$	$x+1$	$x^2+x$	$x^2+x+1$	$x^2+1$
0	0	0	0	0	0	0	0	0	0
$\alpha^0$	1	0	1	x	$x^2$	$x+1$	$x^2+x$	$x^2+x+1$	$x^2+1$
$\alpha^1$	x	0	x	$x^2$	$x+1$	$x^2+x$	$x^2+x+1$	$x^2+1$	1
$\alpha^2$	$x^2$	0	$x^2$	$x+1$	$x^2+x$	$x^2+x+1$	$x^2+1$	1	x
$\alpha^3$	$x+1$	0	$x+1$	$x^2+x$	$x^2+x+1$	$x^2+1$	1	x	$x^2$
$\alpha^4$	$x^2+x$	0	$x^2+x$	$x^2+x+1$	$x^2+1$	1	x	$x^2$	$x+1$
$\alpha^5$	$x^2+x+1$	0	$x^2+x+1$	$x^2+1$	1	x	$x^2$	$x+1$	$x^2+x$
$\alpha^6$	$x^2+1$	0	$x^2+1$	1	x	$x^2$	$x+1$	$x^2+x$	$x^2+x+1$

Multiplication table over  $GF(2^3)$  for  $\alpha = x$  and  $g(x) = x^3+x+1$

5

The seven non-zero rows of the Multiplication table can be used to construct seven distinct Addition tables. Addition table-1 constructed from the first non-zero row of the Multiplication table is illustrated below.

+	0	1	x	$x^2$	$x+1$	$x^2+x$	$x^2+x+1$	$x^2+1$
0	0	1	x	$x^2$	$x+1$	$x^2+x$	$x^2+x+1$	$x^2+1$
1	1	0	$x+1$	$x^2+1$	x	$x^2+x+1$	$x^2+x$	$x^2$
x	x	$x+1$	0	$x^2+x$	1	$x^2$	$x^2+1$	$x^2+x+1$
$x^2$	$x^2$	$x^2+1$	$x^2+x$	0	$x^2+x+1$	x	$x+1$	1
$x+1$	$x+1$	x	1	$x^2+x+1$	0	$x^2+1$	$x^2$	$x^2+x$
$x^2+x$	$x^2+x$	$x^2+x+1$	$x^2$	x	$x^2+1$	0	1	$x+1$
$x^2+x+1$	$x^2+x+1$	$x^2+x$	$x^2+1$	$x+1$	$x^2$	1	0	x
$x^2+1$	$x^2+1$	$x^2$	$x^2+x+1$	1	$x^2+x$	$x+1$	x	0

Addition table-1 over  $GF(2^3)$  for  $\alpha = x$  and  $g(x) = x^3+x+1$

10

We construct a subset  $\{b^{(q)}\}_i$  corresponding to each coset  $\{c^{(m)}\}_i$  by concatenating the sequences of  $\{c^{(m)}\}_i$  according to the rows of the Addition table  $A(2^3)$ , where  $q = p^s = 2^3$ .

This procedure is facilitated by assigning the integer residue class  $Z_{m=8} = \{0, 1, 2, 3, 4, 5, 6,$

7} to the polynomial residue class  $Z_{p=2}[x] = \{1, x, x^2, x+1, x^2+x, x^2+x+1, x^2+1\}$  according to

the sequential mapping  $0 \rightarrow 0, 1 \rightarrow 1, x \rightarrow 2, x^2 \rightarrow 3, x+1 \rightarrow 4, x^2+x \rightarrow 5, x^2+x+1 \rightarrow 6$  and  $x^2+1 \rightarrow 7$ . Then the  $i$ -th subset  $\{b^{(8)}\}_i$  is illustrated below.

$\{b^{(8)}\}_i$	$i$ -th Subset for $0 \leq i \leq 7$
$\{b_k^{(0)}\}_i$	$\{c_n^{(0)}\}_i \{c_n^{(1)}\}_i \{c_n^{(2)}\}_i \{c_n^{(4)}\}_i \{c_n^{(3)}\}_i \{c_n^{(6)}\}_i \{c_n^{(7)}\}_i \{c_n^{(5)}\}_i$
$\{b_k^{(1)}\}_i$	$\{c_n^{(1)}\}_i \{c_n^{(0)}\}_i \{c_n^{(3)}\}_i \{c_n^{(5)}\}_i \{c_n^{(2)}\}_i \{c_n^{(7)}\}_i \{c_n^{(6)}\}_i \{c_n^{(4)}\}_i$
$\{b_k^{(2)}\}_i$	$\{c_n^{(2)}\}_i \{c_n^{(3)}\}_i \{c_n^{(0)}\}_i \{c_n^{(6)}\}_i \{c_n^{(1)}\}_i \{c_n^{(4)}\}_i \{c_n^{(5)}\}_i \{c_n^{(7)}\}_i$
$\{b_k^{(3)}\}_i$	$\{c_n^{(4)}\}_i \{c_n^{(5)}\}_i \{c_n^{(6)}\}_i \{c_n^{(0)}\}_i \{c_n^{(7)}\}_i \{c_n^{(2)}\}_i \{c_n^{(3)}\}_i \{c_n^{(1)}\}_i$
$\{b_k^{(4)}\}_i$	$\{c_n^{(3)}\}_i \{c_n^{(2)}\}_i \{c_n^{(1)}\}_i \{c_n^{(7)}\}_i \{c_n^{(0)}\}_i \{c_n^{(5)}\}_i \{c_n^{(4)}\}_i \{c_n^{(6)}\}_i$
$\{b_k^{(5)}\}_i$	$\{c_n^{(6)}\}_i \{c_n^{(7)}\}_i \{c_n^{(4)}\}_i \{c_n^{(2)}\}_i \{c_n^{(5)}\}_i \{c_n^{(0)}\}_i \{c_n^{(1)}\}_i \{c_n^{(3)}\}_i$
$\{b_k^{(6)}\}_i$	$\{c_n^{(7)}\}_i \{c_n^{(6)}\}_i \{c_n^{(5)}\}_i \{c_n^{(3)}\}_i \{c_n^{(4)}\}_i \{c_n^{(1)}\}_i \{c_n^{(0)}\}_i \{c_n^{(2)}\}_i$
$\{b_k^{(7)}\}_i$	$\{c_n^{(5)}\}_i \{c_n^{(4)}\}_i \{c_n^{(7)}\}_i \{c_n^{(1)}\}_i \{c_n^{(6)}\}_i \{c_n^{(3)}\}_i \{c_n^{(2)}\}_i \{c_n^{(0)}\}_i$

- 5 Then, a set of Orthogonal Structured Codes  $\{s^{(64)}\}$  which contains 64 orthogonal sequences,  $\{s_k^{(i)}\}$ , each of length 64 is constructed by sequentially concatenating the subsets  $\{b^{(8)}\}_i$  for  $i = 0, 1, 2, 3, 4, 5, 6$  and 7 as illustrated below.

[illegible]

[illegible]

For each primitive element  $\alpha$  we can construct a total of seven distinct sets of Orthogonal Structured Codes from the same seed set because seven distinct Addition tables can be derived from any one primitive element. While the sequences are orthogonal within each set they are not orthogonal between sets. However, the inphase crosscorrelation value between sequences belonging to different sets derived from the same primitive element is always equal to  $N^{1/2}$  (i.e. 8 in this case) since the corresponding Addition tables are guaranteed to have only one coincident element per column. Furthermore, since there are exactly  $\phi(p^s-1) = \phi(2^3-1) = 6$  primitive elements, corresponding to the residue polynomials in variable  $x$  modulo  $g(x)$ , then the total number of sets of Orthogonal Structured Codes that can be constructed from each primitive polynomial is 42 (i.e.  $6 \times 7$ ). And since there are exactly  $\phi(p^s-1)/s = \phi(2^3-1)/3 = 2$  primitive polynomials of degree  $s = 3$  in  $GF(2^3)$ , which

are  $g(x) = x^3 + x + 1$  and  $g(x) = x^3 + x^2 + 1$ , then it is possible to construct a total of 84 (i.e.  $2 \times 6 \times 7$ ) distinct sets of Orthogonal Structured Codes from one seed set. In summary, when  $m = p^s = w$  then there are  $\phi(p^s - 1)$ 's primitive polynomials of degree  $s$  in  $GF(p^s)$  each with  $\phi(p^s - 1)$  primitive elements each with  $p^s - 1$  distinct Addition tables. Consequently, the total number of distinct sets of Orthogonal Structured Codes that can be constructed from a common seed set for the condition  $m = w$  is given by

$$\frac{\phi^2(p^s - 1)}{s} \times (p^s - 1).$$

Since the number of orthogonal seed sets available is large when  $m = w > 4$  then the overall numbers of sets of Orthogonal Structured Codes that can be constructed is very large indeed. For example, the following table illustrates six distinct orthogonal seed sets each of which can be used to construct a set of 64 Orthogonal Structured Codes. The table is by no means exhaustive and many more orthogonal seed sets containing  $m = 8$  sequences each of length  $w = 8$  exist. The example shown includes an orthogonal construction on the two m-sequences of length seven, a set of Walsh codes taken from an  $8 \times 8$  Hadamard matrix, an  $8 \times 8$  set of orthogonal Gold sequences and two arbitrary  $8 \times 8$  sets of orthogonal sequences. For the example being illustrated a total of 504 distinct sets of Orthogonal Structured Codes each containing 64 orthogonal sequences of length 64 could be constructed using the six orthogonal seed sets identified. Clearly, such sequences are ideal for cellular mobile application where a large number of sets of sequences with low correlation values are required.

$\{a^{(8)}\}_i$	m-seq. Set 1	m-seq. Set 2	Walsh Codes	Orthogonal Gold Codes	Arbitrary Set 1	Arbitrary Set 2
$\{a_n^{(0)}\}_i$	+++++---	+++++---	+++++++	++-+---+	+++--+--	++-+---+
$\{a_n^{(1)}\}_i$	++-+---+	++-+---+	+-+---+-	+---++++	++-+---+	+-+---+-
$\{a_n^{(2)}\}_i$	+-+---+-	+-+---+-	++-+---+	++-+---+	+-+---+-	+-+---+-
$\{a_n^{(3)}\}_i$	-+---++-	-+---++-	+-+---+-	+++--+--	-+---++-	-+---++-
$\{a_n^{(4)}\}_i$	+-+---+-	+-+---+-	+++++++	++-+---+	+++++++	+++++++
$\{a_n^{(5)}\}_i$	---+++-+	---+++-+	+-+---+-	+++++++	+-+---+-	+-+---+-
$\{a_n^{(6)}\}_i$	-+---++-	-+---++-	++-+---+	++-+---+	++-+---+	++-+---+
$\{a_n^{(7)}\}_i$	-----	-----	+-+---+-	++-+---+	+++++++	+++++++

In summary, the set of Orthogonal Structured Codes constructed in this example are cyclically distinct. The term cyclically distinct is taken to mean that every sequence in the set is not a cyclical shift of any other sequence within the set and hence each sequence is periodic in  $N = 64$ . This property is realised because the rows and columns of each

5 Addition table are distinct. In general, it is conjectured that when  $p \geq 2$  and  $s \geq 3$  the Addition tables over  $GF(p^s)$  will always be distinct and hence the resulting sets of Orthogonal Structured Codes will always be cyclically distinct. This property is specifically beneficial when the sequences are used in multipath since they will remain 'orthogonal' in multipath. This is in contrast to sets of Walsh Codes which are not

10 cyclically distinct and hence do not remain orthogonal in multipath unless covered or masked by another pseudorandom sequence. When  $p = 2$  and  $s = 2$  the rows and columns of the Addition tables over  $GF(4)$  modulo  $g(x) = x^2 + x + 1$  are not distinct (see the construction example given for Condition 3). It is conjectured that this is the only incident when the Addition tables are not distinct. However, if the crosscorrelation condition is

15 relaxed between sets belonging to different Addition table derived from the same primitive element, then for this case an alternative form of the Addition table can be used which involves a rotation or exchange of the elements as illustrated below.

+		0	$\alpha^0$	$\alpha^1$	$\alpha^2$
		0	1	x	x+1
0	0	0	1	x	x+1
$\alpha^0$	1	1	0	x+1	x
$\alpha^1$	x	x	x+1	0	1
$\alpha^2$	x+1	x+1	x	1	0

Addition table over  $GF(2^2)$  for  $\alpha = x$  and  $g(x) = x^2 + x + 1$

20

Modified Addition table based on $A(2^2)$ for $\alpha = x$			
0	1	x	x+1
1	x+1	0	x
x	0	x+1	1
x+1	x	1	0

Alternative Addition table over  $GF(2^2)$  for  $\alpha = x$  and  $g(x) = x^2 + x + 1$

- 44 -

The alternative Addition table might be used in a spread spectrum communication system where a single set is deployed once, thereby avoiding crosscorrelation with other sets, while ensuring that the sequences of the set deployed are cyclically distinct thereby  
 5 guaranteeing 'orthogonality' in multipath. If several sets of Orthogonal Structured Codes are to be deployed simultaneously then the alternative Addition table is not preferable.

Using Structured Codes in a lightwave spread spectrum communication system is achieved by unipolar-bipolar correlation techniques. In general, unipolar-bipolar correlation  
 10 introduces a disturbing term, namely an offset that can be removed by AC coupling the photodetector to the receiver preamplifier. The offset is caused by the one-zero imbalance of the sequences as well as the number of simultaneous sequence transmissions in the case of CDMA. In applications where DC coupling of the photodetector is needed, the off-set can be removed by using either balanced sequences or by using a complementary (second)  
 15 channel that generates a differential signaling format; nominally the second channel being provided by wavelength division multiplexing techniques. Balanced Structured Codes are illustrated hereinafter for lightwave communication. However, Orthogonal Structured Codes may also be used to realise a differential unipolar-bipolar signaling scheme without the need for a second physical channel.

20

A set of Balanced Structured Codes can be constructed from a balanced seed set. The term balanced seed set is taken to mean that every sequence in the seed set has an equal number of "+1" and "-1" elements. When the seed set is balanced the resulting set of Structured Codes is also balanced. Sets of Structured Codes that are balanced have been called  
 25 Balanced Structured Codes. Hence, the identification of balanced seed sets is specifically relevant to the generation of Balanced Structured Codes. A systematic way of constructing Balanced Structured Codes is also based on the use of a binary sequence  $\{a_n\} = (a_0, a_1, a_2, \dots, a_{w-1})$  of length  $w$  that is cyclically distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition

30

$$R(\tau) = \begin{cases} w & \text{for } \tau = 0 \\ \pm 1 & \text{for } \tau \neq 0 \end{cases}$$

Firstly, a set of sequences is constructed from the  $w$  left or right cyclical shifts of  $\{a_n\}$ . Secondly, if  $R(\tau) = -1$  for  $\tau \neq 0$  then an additional sequence element equal to  $\{-1\}$  is appended to each sequence in the set. Alternatively, if  $R(\tau) = +1$  for  $\tau \neq 0$  then an additional sequence element equal to  $\{+1\}$  is appended to each sequence in the set. The resulting set of sequences thus form a balanced seed set. Examples of sequences that are quasi-balanced and fulfill the optimal periodic autocorrelation condition include all m-sequences, the binary Barker sequences  $(++-)$ ,  $(+++--+-)$  and  $(++++--+-+)$ , Legendre sequences when  $w = 4^{k-1}$  for integer  $k$  and certain GMW sequences. Other binary sequences that fulfill these conditions do exist. The procedure for constructing a balanced seed set when  $\{a_n\}$  is cyclically distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition is illustrated by way of example below for  $\{a_n\} = (+++-+--)$ , i.e. an m-sequence. In this example we note that  $m = 7$  while  $w = 8$ .

$\{a^{(7)}\}$	Seed Set
$\{a_n^{(0)}\}$	++++----
$\{a_n^{(1)}\}$	+++-----
$\{a_n^{(2)}\}$	++-----+
$\{a_n^{(3)}\}$	+-+-----
$\{a_n^{(4)}\}$	---+-----
$\{a_n^{(5)}\}$	----+-----
$\{a_n^{(6)}\}$	-----+---

15

Another systematic way to construct a set of Balanced Structured Codes is to use a small set of Balanced Structured Codes as the seed set in the construction of a larger set of Balanced Structured Codes.

20 Algorithms are thus realised for constructing the Structured Codes. Additionally, specific sets of sequences have been identified for use in spread spectrum communication techniques.

25 Applications of the signature sequences will now be described with reference to specific transmitter and receiver architectures. Usually, the transmitter and receiver are combined at each end of the communication path for bi-directional communication. Thus, by way of example the transceiver design is based on an  $M$ -ary bi-orthogonal keying scheme. An

alternative example would be an  $M$ -ary orthogonal keying scheme. In an  $M$ -ary bi-orthogonal keying scheme one of  $M$  possible symbols is transmitted during each symbol interval, where  $M > 2$ . Each symbol represents a co-ordinate in a  $K$ -dimensional signal space using  $K = M/2$  orthonormal basis functions. In  $M$ -ary bi-orthogonal keying the symbol set consists of  $M/2$  orthonormal basis functions and their complements. For the transceiver designs presented, the orthonormal basis functions are chosen from sets of Orthogonal Structured Codes. Consequently, spectrum spreading and  $M$ -ary transmission are combined in a single bandwidth efficient modulation scheme. Though  $M$ -ary bi-orthogonal keying is an established digital modulation scheme, the use of Orthogonal Structured Codes as orthonormal basis functions is completely new.

In the description which follows the notation adopted is:  $\{\phi_n^{(j)}\}$  denotes the  $j$ -th Orthogonal Structured Code with elements  $\phi_n \in \{\pm 1\}$ ;  $\{\phi_n^{(j)}\}$  denotes the unipolar version of  $\{\phi_n^{(j)}\}$  with elements  $\phi_n \in \{1, 0\}$ ; and  $\phi(t)$  and  $\phi(t)$  denote bipolar and unipolar waveform versions of  $\{\phi_n^{(j)}\}$  and  $\{\phi_n^{(j)}\}$ , respectively. In addition,  $d(t)$  and  $D(t)$  denote unit amplitude, rectangular bipolar and unipolar data waveforms, respectively.

In this general arrangement, the transmitter architecture is firstly described with reference to Figure 1. Unipolar binary data  $D(t)$  is fed into a  $1:k$  multiplexer at rate  $1/T$ , where  $k = \log_2 M$ . At the multiplexer output, the  $(k-1)$  most-significant bits (MSB) are used to choose one from  $K = M/2 = 2^{k-1}$  sequences thereby determining the symbol waveform. The least significant bit (LSB) determines whether or not the sequence is complemented thereby realising the other half of the symbol code-book. The resulting symbol waveform is then made available for transmission. The transmitter architecture is based on a standard  $M$ -ary bi-orthogonal keying scheme except that the symbol waveforms have the dual functionality of spreading the spectrum and acting as orthonormal basis functions. This is possible because the sequences are taken from sets of Orthogonal Structured Codes. In general, this may be expressed by

$$\{\phi_n^{(j)}\} = \{s_n^{(j)}\}$$

for  $0 \leq j \leq K-1$  and the maximum value of  $K$  is  $N$ .



Figure 2 is a schematic diagram of a receiver design. For the  $M$ -ary transmitter architecture presented above, the corresponding receiver consists of a bank of  $K$ -correlators matched to the orthonormal basis functions  $\phi(t)$ , where  $K = M/2 = 2^{k-1}$ . The outputs from the correlators are passed to samplers and are sampled at time  $t = kT$  before being fed into a decision logic block where a maximum likelihood detection of the data transmitted is performed. For the  $M$ -ary bi-orthogonal scheme this involves a search for the greatest magnitude peak at the outputs of the bank of  $K$ -correlators and subsequently the polarity of the greatest magnitude peak. This information can then be used to uniquely identify the transmitted symbol and hence the corresponding data bits. The logic output is  $\hat{D}(t)$ , the estimate of  $D(t)$  the original unipolar binary data inputted to the transmitter.

In a first embodiment, a wireless communication system is disclosed. The transmitter and receiver architectures described with reference to Figures 1 and 2 are adapted for use with coded signals based on Orthogonal Structured Codes. Such generalised architectures may be used in any spread spectrum signaling scheme. For example, in a radio communications system the output of the transmitter shown in Figure 1 can be directly carrier modulated using either amplitude, frequency or phase modulation techniques. In a wireless infrared communication system based on unipolar-bipolar correlation techniques, Figures 3 and 4 show schematic diagrams of the transmitter and receiver architectures incorporating the electro-optic interfaces. At the transmitter the same  $M$ -ary bi-orthogonal keying scheme is used to generate unipolar symbol waveforms which directly control a drive circuit that switches a lightwave source, such as a Light Emitting Diode or Laser Diode, on and off. As in the generalised architecture of Figure 1, the orthonormal basis functions are obtained from sets of Orthogonal Structured Codes.

At the receiver shown in Figure 4, the optical signal is detected by a photodiode or an array of photodiodes and amplified by a broadband transimpedance amplifier before being fed into a bank of  $K$ -correlators. The correlator outputs are passed through samplers to be sampled at time  $t = kT$  and then fed into a decision logic block that implements a maximum likelihood detection of the data transmitted.

When the photodiode is DC coupled to the receiver, the unipolar-bipolar correlation technique presented above generates an off-set if the spreading sequences are imbalanced. One method to remove this inherent off-set is to use Balanced Structured Codes as orthonormal basis functions. However, the performance of a full set of Balanced Structured Codes is inferior to the performance of a full set of Orthogonal Structured Codes. If the photodiode is AC coupled to the receiver then Orthogonal Structured Codes may be used without introducing a sequence dependent offset. In applications where DC coupling is required, the offset produced by imbalanced sequences can be removed efficiently by a differential unipolar-bipolar signaling format. Figure 5 illustrates a schematic diagram of a differential unipolar-bipolar signaling scheme. In addition to removing the off-set effect, a differential unipolar-bipolar signaling scheme removes common mode interference. This is particularly useful for combating artificial ambient light interference, such as that produced by electronic-ballast-driven lamps, in an infrared wireless transmission embodiment.

Bipolar data  $d(t)$  at a rate of  $1/T$  and its inverse  $-d(t)$  are spread by multiplication with the orthonormal basis functions  $\phi_j^c(t)$  and  $\phi_j^s(t)$ , respectively, where  $\phi_j^c(t)$  and  $\phi_j^s(t)$  are an orthogonal pair of spreading sequences. In practice,  $\phi_j^c(t)$  and  $\phi_j^s(t)$  can be selected from a set of Orthogonal Structured Codes. As an Orthogonal Structured Code  $\{s_n^{(j)}\}$  and its reverse sequence  $\{s_n^{(j)*}\}$  form an orthogonal pair, it is recommended that  $\phi_j^c(t) \equiv \{s_n^{(j)}\}$  and  $\phi_j^s(t) \equiv \{s_n^{(j)*}\}$  are chosen to result in an efficient allocation of sequences. The orthogonal pair of signals are then converted from bipolar to unipolar format using Level Shifters, summed together and then transmitted on a unipolar channel such as a lightwave medium.

At the receiver, the total received signal  $s(t)$  is directly multiplied in parallel by the bipolar orthonormal basis functions  $\phi_j^c(t)$  and  $\phi_j^s(t)$ . The outputs from the multipliers are differenced and the resulting difference signal is then integrated over the symbol period  $T$ . In a differential unipolar-bipolar signaling scheme, the in-phase value of the correlator output is the same as that obtained when a normal bipolar-bipolar signaling format is used.

The transmitter and receiver architectures shown in Figures 3 and 4 may be converted from a unipolar-bipolar signaling format to a differential unipolar-bipolar signaling format by augmenting the  $M$ -ary bi-orthogonal keying scheme with the circuits shown in Figure 5.

Consequently, in the receiver two multipliers are required per branch. A schematic diagram of an  $M$ -ary bi-orthogonal keying scheme incorporating differential signaling is shown in Figure 6 while a schematic diagram of the corresponding receiver is shown in Figure 7. In the transmitter, the differential symbol waveforms drive separate lightwave sources. Consequently, the summation of differential signals takes place on the lightwave channel. This configuration has the advantage that the drive circuits remain digital thereby avoiding non-linearity problems in the transmitter.

For a given sequence length  $N$ , the spectral efficiency of a spread spectrum communication system can be substantially increased by using two or more distinct sets of Orthogonal Structured Codes in one transceiver. Figures 8 and 9 show schematic diagrams of a transmitter and receiver, respectively, that use two distinct orthogonal code sets in an  $M$ -ary bi-orthogonal keying scheme. That is, the transceiver consists of two  $M$ -ary bi-orthogonal keying schemes combined in parallel but using two distinct code sets. In this case, the capacity of the communication link is doubled. In the transmitter, shown in Figure 8, unipolar binary data  $D(t)$  is fed into a  $1:2k$  multiplexer at rate  $1/T$ , where  $k = \log_2 M$ . The first  $k$  multiplexed data bits feed one branch of the  $M$ -ary bi-orthogonal keying scheme while the second  $k$  multiplexed data bits feed the other branch of the  $M$ -ary bi-orthogonal keying scheme. The receiver, shown in Figure 9, consists of two banks of  $K$ -correlators; one matched to the first code set while the other bank is matched to the second code set. Two distinct maximum likelihood detectors are used to detect the data belonging to each parallel  $M$ -ary bi-orthogonal scheme. Once detected, the data from each branch is combined using a  $2k:1$  multiplexer. Ideally, the distinct code-sets should be orthogonal in order to avoid any crosscorrelation interference when two symbol waveforms are transmitted and received in parallel. In practice, the distinct code sets are not mutually orthogonal and hence cross-interference occurs. However, code sets can be chosen from the large number of Orthogonal Structured Codes such that the crosscorrelation interference does not cause transmission errors. An example of two such code sets for  $N = 16$  are the Orthogonal Structured Codes constructed on the seed sequence  $\{a_n\} = (+, +, +, -)$  using two distinct Addition tables derived from the same Multiplication table.

It is considered preferable, although not essential, that the spreading sequences in a differential unipolar-bipolar signaling format are orthogonal. If the only requirement is to remove a sequence dependent off-set, then any pair of periodic binary sequences  $\{a_n\}$  and  $\{b_n\}$  can be used providing that they have the same  $\{1,0\}$  chip imbalance. This condition  
5 may be satisfied by using a sequence pair consisting of the sequence  $\{a_n\}$  and its reverse sequence  $\{b_n\} = \{\bar{a}_n\}$ . A potential disadvantage of using a non-orthogonal sequence pair is that crosscorrelation interference is produced at the receiver. However, by an appropriate choice of the initial phase of the sequence, the crosscorrelation interference can be made constructive rather than destructive. Figure 10 shows a schematic diagram of a differential  
10 unipolar-bipolar signaling scheme applicable to any periodic binary sequence.

In a first exemplifying embodiment, an infrared communications system for a wireless local area network comprises a plurality of remote communication terminals, each terminal including a transmitter circuit having means for generating and encoding signature  
15 sequences for spread spectrum communication techniques, a means for transmitting coded infrared signals and a receiver circuit for receiving coded infrared signals having means for decoding signature sequences in a spread spectrum communication system.

In this embodiment each remote communication terminal comprises an infrared transceiver  
20 that can use either the transmitter and receiver pair shown in Figures 3 and 4, respectively, or the transmitter and receiver pair shown in Figures 6 and 7, respectively. For the transceiver implemented according to Figures 3 and 4, binary data is fed into a  $1:k$  multiplexer from which the  $k-1$  MSB are used to choose one from  $K$  sequences which may or may not be complemented by the LSB. The code set is chosen from a set of Orthogonal  
25 Structured Codes. The symbol waveform thus generated is used to intensity modulate a lightwave source such as a Light Emitting Diode or a Laser Diode. At the receiver a photosensitive detector, for example, a photodiode or an array of photodiodes, detects the lightwave signal. The resulting photocurrent is amplified and a bank of  $K$ -correlators generates  $K$  matched filter samples. The  $K$  samples are fed into a maximum likelihood  
30 detector circuit that detects the  $k$  transmitted data bits and converts them into a single serial bit stream, which is an estimate of the transmitted data. Each receiver contains a means of

synchronisation that aligns the received signal with the locally generated spreading sequences used in the bank of  $K$ -correlators.

For the transceiver implemented according to Figures 6 and 7, unipolar binary data  $D(t)$  is fed into an  $1:k$  multiplexer. The  $k-1$  MSB feed two distinct code sets that are mutually orthogonal; i.e. code set  $\{\Phi\}^c$  and  $\{\Phi\}^s$  where  $\{\Phi\}^c$  is orthogonal to  $\{\Phi\}^s$ . The  $k-1$  MSB are used to choose one from  $K$  sequences in both code sets denoted by  $\{\Phi_n^{(j)}\}^c$  and  $\{\Phi_n^{(j)}\}^s$ . The LSB when logic "Hi" will not complement  $\{\Phi_n^{(j)}\}^c$  but will complement  $\{\Phi_n^{(j)}\}^s$  and visa versa when the LSB is logic "Lo". Each symbol waveform is used to intensity modulate a separate lightwave source such as a Light Emitting Diode or a Laser Diode. The differential symbol waveform is formed by summation of the parallel symbol waveforms in the lightwave medium. Alternatively, the parallel symbol waveforms can be summed prior to electro-optic conversion and the resulting differential symbol waveform used to drive a single lightwave source. At the receiver a photosensitive detector, for example a photodiode or an array of photodiodes, detects the lightwave signal. The resulting photocurrent is amplified and a bank of  $K$  differential correlators generate  $K$  matched filter samples. A differential correlator consists of two parallel correlators, one for each possible pair of symbol waveforms, whose outputs are subtracted. The  $K$  samples are fed into a maximum likelihood detector circuit that detects the  $k$  transmitted data bits and converts them into a single serial bit stream, which is an estimate of the transmitted data. Each receiver contains a means of synchronisation that aligns the received signal with the locally generated spreading sequences used in the bank of  $K$  differential correlators.

The advantages of the techniques used in the above embodiment are:

25

- (1) When combined with  $M$ -ary bi-orthogonal keying, sets of Orthogonal Structured Codes give bandwidth efficient modulation schemes that are robust against narrow band interference and multipath propagation effects.
- (2) When differential unipolar-bipolar signaling is embedded within a lightwave spread spectrum communication system then common mode interfering signals are removed. In a lightwave spread spectrum system this has the advantage of removing the DC offset caused by the sequence imbalance. In a wireless lightwave spread

30

- 52 -

spectrum system this has the added advantage of reducing the degradation in system performance caused by interference from ambient artificial light.

- (3) When used as direct spreading sequences, sets of Orthogonal Structured Codes remain orthogonal under multipath condition and in general possess excellent autocorrelation and crosscorrelation properties.
- (4) When used as direct spreading sequences, sets of Orthogonal Structured Codes aid synchronisation between transceiver pairs because they form Complementary Sets.

In a second exemplifying embodiment, a radio communication system for a wireless local area network comprises a plurality of remote communication terminals, each terminal including a transmitter circuit having means for generating and encoding signature sequences for spread spectrum communication techniques, a means for transmitting coded radio signals and a receiver circuit for receiving coded radio signals having means for decoding signature sequences in a spread spectrum communication system.

In this embodiment, each remote communication terminal comprises a radio transceiver that uses the transmitter and receiver pair shown in Figures 1 and 2, respectively. At the transmitter, binary data is fed into a  $1:k$  multiplexer from which the  $k-1$  MSB are used to choose one from  $K$  sequences that may or may not be complemented by the LSB. The code set is chosen from a set of Orthogonal Structured Codes. The symbol waveform generated modulates a radiowave carrier for transmission. At the receiver, the radiowave signal is detected via an antenna and subsequently is demodulated in order to remove the radiowave carrier. A bank of  $K$ -correlators generate  $K$  matched filter samples. The  $K$  samples are fed to a maximum likelihood detector circuit that detects the  $k$  transmitted data bits and converts them into a single serial bit stream, which is an estimate of the transmitted data. Each receiver contains a means of synchronisation that aligns the received signal with the locally generated spreading sequences used in the bank of  $K$ -correlators.

The advantages of the techniques used in the above embodiment are:

- 53 -

- (1) When combined with  $M$ -ary bi-orthogonal keying, sets of Orthogonal Structured Codes give bandwidth efficient modulation schemes that are robust against narrow band interference and multipath propagation effects.
  - (2) When used as direct spreading sequences, sets of Orthogonal Structured Codes remain orthogonal under multipath condition and in general possess excellent autocorrelation and crosscorrelation properties.
  - (3) When used as direct spreading sequences, sets of Orthogonal Structured Codes aid synchronisation between transceiver pairs because they form Complementary Sets.
- 10 In the above embodiment, common mode interfering signals can be removed by embedding a differential signaling scheme within a radiowave spread spectrum system based on the architectures shown in Figures 6 and 7.

15 In a third exemplifying embodiment, a radio code division multiple access (CDMA) communication system for use, for example, in cellular mobile radio networks, wireless local loop networks, radio packet data networks or satellite networks comprises a plurality of remote communication terminals that send and receive radio signals to and from, respectively, a central base station. Each remote terminal has a transmitter circuit having means for generating and encoding signature sequences for CDMA communication techniques, a means for transmitting coded radio signals and a receiver circuit for receiving coded radio signals having means for decoding signature sequences in a CDMA communication system. Each base station has transmitter circuits having means for generating and encoding signature sequences for CDMA communication techniques, a means for transmitting coded radio signals and receiver circuits for receiving coded radio signals having means for decoding signature sequences in a radio CDMA communication system.

This embodiment generally consists of a centralised access point, connected to a fixed network, and a number of remote terminals within the area of coverage of the access point.

30 This network topology is typical of a cellular mobile radio network, a wireless local loop network or a packet data radio network. Usually, frequency division duplexing is used to separate the uplink and downlink transmissions. However, within either the uplink or

- 54 -

downlink, separation between communication channels is achieved by code division multiple access. The downlink transmitter uses the binary data of a user to sequence inverse key an Orthogonal Structured Code. This process ensures that each user within a cell is orthogonal to every other user within the cell when a full set of Orthogonal Structured Codes are used. A significant advantage of using Orthogonal Structured Codes as opposed to Walsh codes in this application is that the Orthogonal Structured Codes remain orthogonal in multipath where as Walsh codes do not. After sequence inverse keying the symbol waveform modulates a radiowave carrier for transmission. The downlink receiver reverses the operations performed by the downlink transmitter. The radiowave signal is detected by an antenna and demodulated in order to remove the radiowave carrier. The resulting signal consists of the signals intended for all users in the cell. A user's data is recovered by using a matched filter detector matched to the corresponding Orthogonal Structured Code.

A user's uplink transmitter is based on the architecture shown in Figure 1, that is an  $M$ -ary bi-orthogonal keying scheme. Binary data is fed into a  $1:k$  multiplexer from which the  $k-1$  MSB are used to chose one from  $K$  sequences which may or may not be complemented by the LSB. The code set is chosen from a set of Orthogonal Structured Codes. The symbol waveform generated modulates a radiowave carrier for transmission. A user's uplink receiver is based on the architecture shown in Figure 2. The radiowave signal is detected by an antenna and demodulated in order to remove the radiowave carrier. A bank of  $K$ -correlators generate  $K$  matched filter samples. The  $K$  samples are fed to a maximum likelihood detector circuit that detects the  $k$  data bits and converts them into a single serial bit stream which is an estimate of the transmitted data. Each receiver contains a means of synchronisation that aligns the received signal with the locally generated spreading sequences used in the bank of  $K$ -correlators.

The advantages of the techniques used in the above embodiment are:

- (1) When combined with  $M$ -ary bi-orthogonal keying, sets of Orthogonal Structured Codes give bandwidth efficient modulation schemes that are robust against narrow band interference and multipath propagation effects.



- 55 -

- (2) When used as direct spreading sequences, sets of Orthogonal Structured Codes remain orthogonal under multipath condition and in general possess excellent autocorrelation and crosscorrelation properties.
- (3) When used as direct spreading sequences, sets of Orthogonal Structured Codes aid  
5 synchronisation between transceiver pairs because they form Complementary Sets.

In the above embodiment, common mode interfering signals can be removed by embedding a differential signaling scheme within a radiowave spread spectrum system based on the architectures shown in Figures 6 and 7. This can be done on both the uplink  
10 and downlink.

In a fourth exemplifying embodiment, a lightwave CDMA communication system for an optical fibre local area network comprises a plurality of remote communication terminals that transmit and receive lightwave signals and which are interconnected by optical fibre.  
15 Each terminal has a transmitter circuit having means for generating and encoding signature sequences for lightwave CDMA communication techniques, a means for transmitting coded lightwave signals and a receiver circuit for receiving coded lightwave signals having means for decoding signature sequences in a lightwave CDMA communication system.

20 The term "lightwave" is taken to mean electromagnetic radiation within the ranges of visible light and near and far infrared light.

In this embodiment each communication terminal comprises a lightwave transceiver based on the transmitter and receiver architecture shown in Figure 5. In general, lightwave  
25 transceivers are interconnected by a shared lightwave medium such as optical fibre. At the transmitter binary data is converted from a single serial bit stream into two parallel differential bit streams consisting of the original data and its inverse. Each differential bit stream sequence inverse keys a unique spreading code where each unique spreading code is chosen from a set of Orthogonal Structured Codes. Each differential spread spectrum  
30 signal then intensity modulates an individual lightwave source, for example a Light Emitting Diode or a Laser Diode. The two emitted lightwave signals sum on the lightwave transmission medium to produce a differential spread spectrum signal. In an alternative

- 56 -

arrangement the two parallel spread spectrum signals are first summed and the summand intensity modulates a single lightwave source. At the receiver a photosensitive detector, for example a photodiode, detects the lightwave signal. The resulting photocurrent is amplified and a differential correlator generates a matched filter sample. The sample is fed to a  
5 binary threshold detector circuit that detects the serial bit stream, which is an estimate of the transmitted data. It should be noted that a differential signaling scheme may use any code pair to spread the differential data providing that the sequences used have the same {1,0} chip imbalance (see Figure 10). Each receiver contains a means of synchronisation that aligns the received signal with the locally generated spreading sequences used in the  
10 correlator.

The advantages of the techniques used in the above embodiment are:

- 15 (1) When differential unipolar-bipolar signaling is embedded within a lightwave spread spectrum communication system then common mode interfering signals are removed. In a lightwave CDMA system this has the advantage of removing the DC offset caused by sequence imbalance.
  - (2) When used as direct spreading sequences, sets of Orthogonal Structured Codes possess excellent autocorrelation and crosscorrelation properties. Specifically, when  
20 synchronised, the sequences will support  $N$  users where  $N$  is the set size as well as remove the near/far effect.
  - (3) When used as direct spreading sequences, sets of Orthogonal Structured Codes aid synchronisation between transceiver pairs because they form Complementary Sets.
- 25 The sequences presented hereinabove represent a significant development in signature sequences for spread spectrum communication techniques. For example, Orthogonal Structured Codes combine properties of orthogonality for certain well defined cyclical shifts with small autocorrelation and crosscorrelation values for other cyclical shifts. These properties make Orthogonal Structured Codes ideal spreading sequences in a direct  
30 sequence spread spectrum system. Specifically, when synchronised Orthogonal Structured Codes can give a spectral efficiency of 100% while obviating the near/far effect in a non-dispersive channel. However, in a dispersive channel Orthogonal Structured Codes remain

- 57 -

orthogonal unlike the Walsh codes. Significantly, the algorithm described herein is capable of systematically constructing multiple sets of orthogonal sequences for most practical code lengths and beyond. That is, two or more sets of Orthogonal Structured Codes can be constructed for a given sequence length  $N$ . The implication being that such code sets may  
5 be used in parallel in order to give a substantial increase in the capacity of a spread spectrum communication system. In addition, a very useful property of Orthogonal Structured Codes is that they form Complementary Sets of sequences. That is, the aperiodic autocorrelation function of all sequences in a set of Orthogonal Structured Codes sum to zero for every time shift, except the zero shift.

10

It will be seen that the application of these sequences is not limited to infrared wireless communication but may be applied to a wide range of communication techniques which include radiowave as well as lightwave techniques and fixed as well as wireless techniques. A sample application tree is illustrated in Figure 11. Other communication  
15 systems that would particularly benefit from the sequences are cellular mobile radio networks, wireless local loop networks, radio packet data networks, satellite networks and radio local area networks. The use of Structured Codes, specifically Orthogonal Structured Codes, facilitates higher throughput of data for a given bandwidth allowing either a greater number of users or higher data rates for each channel.

20

Another contribution of the present invention is the disclosure of new  $M$ -ary digital transmission architectures based on Orthogonal Structured Codes. These  $M$ -ary architectures combine spectrum spreading with orthonormal basis functions to realise bandwidth efficient transmission schemes that are robust to interference and multipath  
25 propagation effects. General architectures relevant to any spread spectrum or CDMA communication system and specific architectures relevant to infrared wireless systems, radio systems and optical fibre systems are disclosed. In addition, transceiver architectures based on combining independent sets of Orthogonal Structured Codes are disclosed. These architectures can at least double the capacity of conventional spread spectrum  
30 communication systems.

- 58 -

The further contribution to the art is that of differential unipolar-bipolar signalling. This signalling scheme removes the sequence dependent off-set associated with unipolar-bipolar signalling and allows any family of binary signature sequences to be used in a lightwave (unipolar) transmission system. Differential unipolar-bipolar signalling uses code division  
5 of differential data on a single transmission channel. Code division is ideally achieved using Orthogonal Structured Codes, however, any binary code pair can be used providing they have the same {1,0} imbalance.

The sequences are generated by a combination of sequence modulation and concatenation of a selected seed set of sequences. When the seed set is orthogonal then the set of  
10 Structured Codes constructed is also orthogonal. Furthermore, by adopting different Addition tables, other sets of Structured Codes can be constructed.

Using Orthogonal Structured Codes to provide orthonormal basis function while spreading the spectrum at the same time is a significant development in the art of *M*-ary digital  
15 transmission. By combining two or more distinct sets of Orthogonal Structured Codes, spread spectrum communication systems with significantly enhanced capacities can be realised.

The use of code division to separate differential data on a single unipolar (lightwave)  
20 transmission channel is provided by the differential unipolar-bipolar signaling scheme presented above with reference to Figures 5 and 10. The realisation of code-division using any binary sequence and not just orthogonal sequences is a significant development as is the incorporation of a differential unipolar-bipolar signaling scheme into an *M*-ary digital transmission scheme based on Orthogonal Structured Codes.

25 In addition, the Structured Codes presented have beneficial applications in error correction/detection, synchronisation, cryptography, power-line communications, ranging and tomography.

30 The new Structured Codes disclosed in this document have been named Supergold codes and their application to specific systems has been named Supergold coding.

- 59 -

It will be understood that the current invention is not limited to the electromagnetic radiation based carriers such as lightwave carriers (e.g. infrared or visible light) or radio frequency carriers but may be implemented using any suitable carrier. Such suitable alternatives may include, but are not limited to the use of sonic or seismic media in  
5 response to a given application requirement.

It will of course be understood that the invention is not limited to the specific details described herein, which are given by way of example only, and that various modification and alterations are possible within the scope of the invention.

Claims

1. A method for spread spectrum communication using a signature sequence, the signature sequence being generated by performing the steps of:-  
5                   selecting a seed set of sequences of a given size;  
  
                      generating a plurality of cosets from the seed set of sequences;  
  
10                   constructing a subset of sequences by concatenating the sequences of a coset; and  
  
                      constructing a full set of sequences by concatenating subsets of sequences.
- 15   2. A method as claimed in claim 1 wherein the seed set contains binary sequences.
3. A method as claimed in claim 2 in which the binary sequence is cyclically distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition.
- 20   4. A method as claimed in claim 1 in which the seed set contains complex sequences.
5. A method as claimed in any of claims 1 to 4 in which the seed set incorporates a plurality of inner sequences.
- 25   6. A method as claimed in any preceding claim in which the seed set is orthogonal.
7. A method as claimed in any of claims 3 to 6 in which the cosets are generated by multiplying in turn each inner sequence by an element of an associated sequence.
- 30   8. A method as claimed in any preceding claim in which the subset of sequences is constructed by concatenating the sequences of a coset using an addition table.

- 61 -

9. A method as claimed in claim 8 in which the addition table is constructed using powers of a primitive root of the seed set of sequences, the primitive root being determined in accordance with the size of the seed set.
- 5 10. A method as claimed in claim 8 in which the addition table is constructed using powers of a primitive element of the seed set of sequences, the primitive element being determined in accordance with the size of the seed set.
11. A method as claimed in any preceding claim in which the seed set is formed from a plurality of rotated sequences.
- 10 12. A method for producing a structured code for use in spread spectrum data communication comprising the steps of:-
- 15 selecting a seed set of sequences of a given size;
- generating a plurality of cosets from the seed set of sequences;
- constructing a subset of sequences by concatenating the sequences of a coset; and
- 20 constructing a full set of sequences by concatenating subsets of sequences.
13. A method as claimed in claim 12 in which the seed set contains binary sequences.
- 25 14. A method as claimed in claim 12 in which the binary sequence is cyclically distinct, quasi-balanced and satisfies the optimal periodic autocorrelation condition.
15. A method as claimed in claim 12 in which the seed set contains complex sequences.
- 30 16. A method as claimed in any of claims 12 to 15 in which the seed set incorporates a plurality of inner sequences.

17. A method as claimed in any of claims 12 to 16 in which the seed set is orthogonal.
18. A method as claimed in any of claims 12 to 17 in which the cosets are generated by  
5 multiplying in turn each inner sequence by an element of an associated sequence.
19. A method as claimed in any of claims 12 to 18 in which the subset of sequences is constructed by concatenating the sequences of a coset using an addition table.
- 10 20. A method as claimed in claim 19 in which the addition table is constructed using powers of a primitive root of the seed set of sequences, the primitive root being determined in accordance with the size of the seed set.
21. A method as claimed in claim 19 in which the addition table is constructed using  
15 powers of a primitive element of the seed set of sequences, the primitive element being determined in accordance with the size of the seed set.
22. A method as claimed in any of claims 12 to 21 in which the seed set is formed from a plurality of rotated sequences.
- 20 23. An apparatus for constructing and encoding signature sequences for spread spectrum communication techniques, the apparatus comprising:
- a seed set generating means for constructing a seed set of sequences;
- 25 a coset generating means for generating cosets of sequences;
- an expansion means for concatenating sequences of a generated coset according to a predetermined order, to form a subset of sequences for each  
30 coset; and



- 63 -

a set generating means for constructing a full set of sequences by concatenating subsets.

5     24.     An apparatus as claimed in claim 23 in which the seed set generating means comprises a plurality of shift registers, each shift register having an input, a system clock input, logic gates, a plurality of register cells/stages and an output to form a sequence of the seed set.

10    25.     An apparatus as claimed in claim 23 or claim 24 in which the seed set generating means includes a number of linear feedback shift registers.

26.     An apparatus as claimed in any of claims 23 to 25 in which the expansion means comprises:-

15

a plurality of inputs, each input corresponding to a sequence from a coset;

a plurality of multiplexers having associated counters and logic gates;  
a system clock input; and

20

a plurality of outputs to form a subset of sequences.

27.     An apparatus as claimed in any of claims 23 to 26 for decoding signature sequences  
25     in a spread spectrum communications system, the apparatus comprising:

means for receiving coded signals;

means for generating sequence functions;

30

means for combining received coded signals with sequence functions to produce despread signal outputs;

- 64 -

means for combining the despread signal outputs to generate a data stream;  
and

5                   logic circuitry for analysing the data stream.

28.   A data transmission system having a transmitter and a receiver, the transmitter incorporating means for transmitting data using a signature sequence and the receiver formed for receiving and decoding data transmitted using a signature  
10                   sequence, the signature sequence being generated by performing the steps of:-

                  selecting a seed set of sequences of a given size;

                  generating a plurality of cosets from the seed set of sequences;

15

                  constructing a subset of sequences by concatenating the sequences of a coset; and

                  constructing a full set of sequences by concatenating subsets of sequences.

20

29.   An electromagnetic radiation or sonic communications system for a communications network comprising a plurality of remote communication terminals, each terminal including a transmitter circuit having means for generating  
25                   and encoding signature sequences for spread spectrum communication techniques by performing the steps of selecting a seed set of sequences of a given size, generating a plurality of cosets from the seed set of sequences, constructing a subset of sequences by concatenating the sequences of a coset and constructing a full set of sequences by concatenating subsets of sequences, the transmitter circuit  
30                   also having, a means for transmitting coded signals and a receiver circuit for receiving coded signals the receiver circuit having means for decoding signature sequences in a spread spectrum communication system.

- 65 -

30. An electromagnetic radiation or sonic communications system as claimed in claim 29 in which the communications network uses a radio frequency carrier.
- 5 31. An electromagnetic radiation or sonic communications system as claimed in claim 29 in which the communications network uses an ultrasound carrier.
32. An electromagnetic radiation or sonic communications system as claimed in claim 29 in which the communications network uses a seismic carrier.
- 10 33. An electromagnetic radiation or sonic communications system as claimed in claim 29 in which the communications network uses a lightwave carrier.
34. An electromagnetic radiation or sonic communications system as claimed in claim 15 33 in which the communications network uses an infrared carrier.
35. An electromagnetic radiation or sonic communications system as claimed in claim 20 33 or 34 in which the receiver circuit incorporates a photodetector, the photodetector having an associated coupling means communicating with a receiver preamplifier.
36. An electromagnetic radiation or sonic communications system as claimed in claim 35 in which the coupling means is formed for differential signal recognition.
- 25 37. An electromagnetic radiation or sonic communications system as claimed in any of claims 29 to 36 in which the seed set is a balanced seed set.
38. An electromagnetic radiation or sonic communications system as claimed in any of 30 claims 29 to 37 in which the encoding signature sequences incorporates orthogonal structured codes.

39. A communications method for transmission of data in a network using a unipolar-bipolar signaling scheme, the scheme having code division means for separating differential data on a unipolar or bipolar transmission channel.
- 5 40. A communications method for transmission of data as claimed in claim 39 in which the code division means utilises a binary sequence.
41. A communications method for transmission of data as claimed in claim 40 in which the binary sequence is orthogonal.
- 10 42. A communications method for transmission of data as claimed in any of claims 39 to 41 incorporating means for integrating an  $M$ -ary digital transmission scheme based on orthogonal structured codes.

1/11

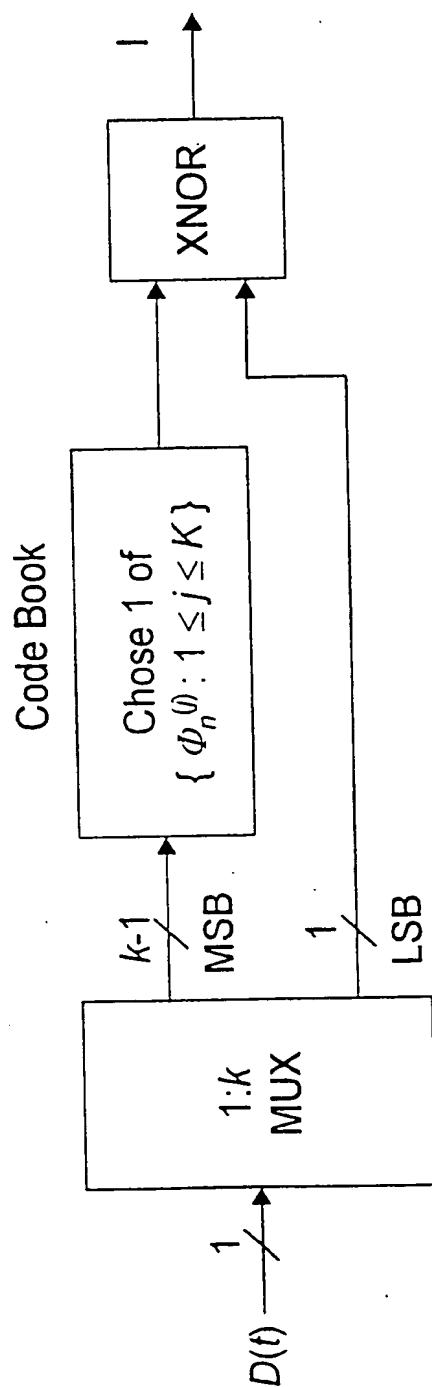


Figure 1

2/11

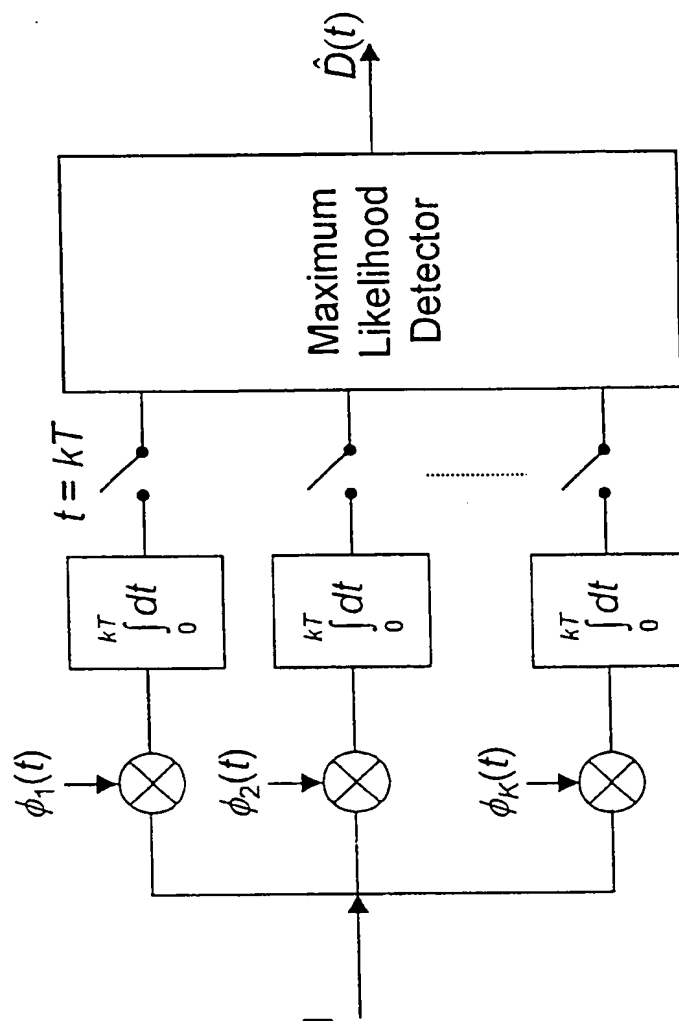


Figure 2

3/11

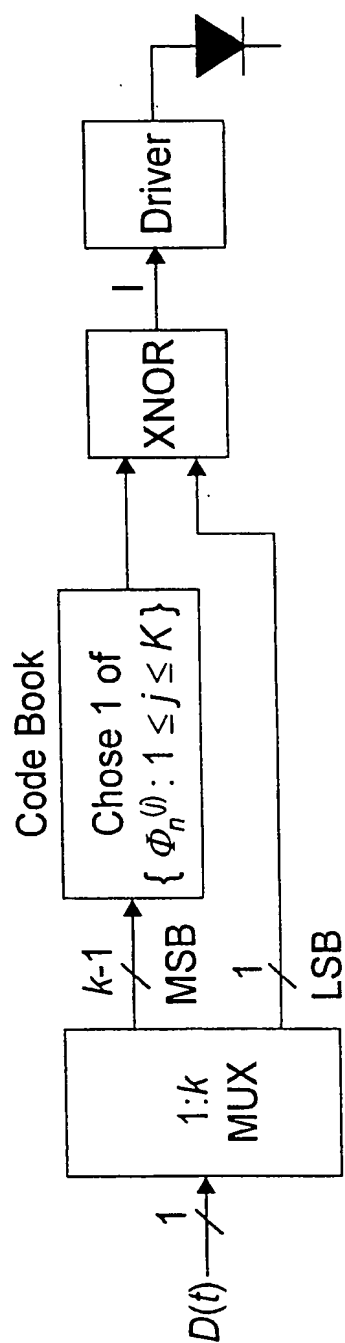


Figure 3

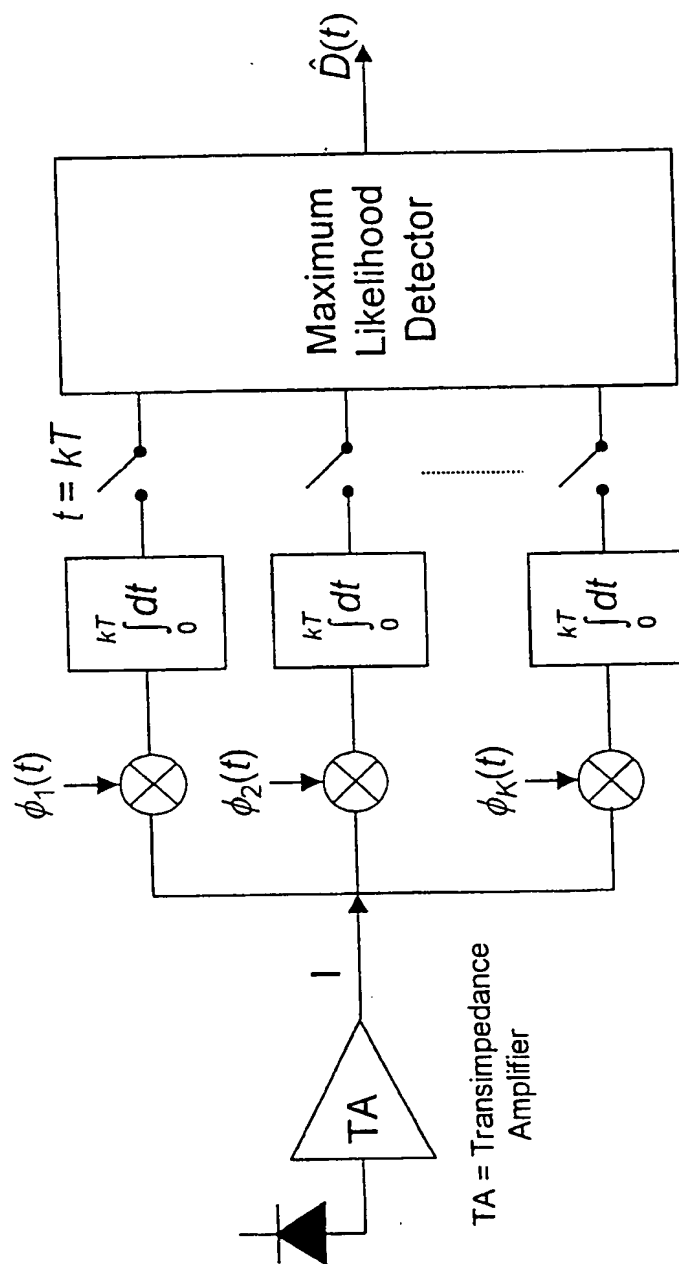


Figure 4



5/11

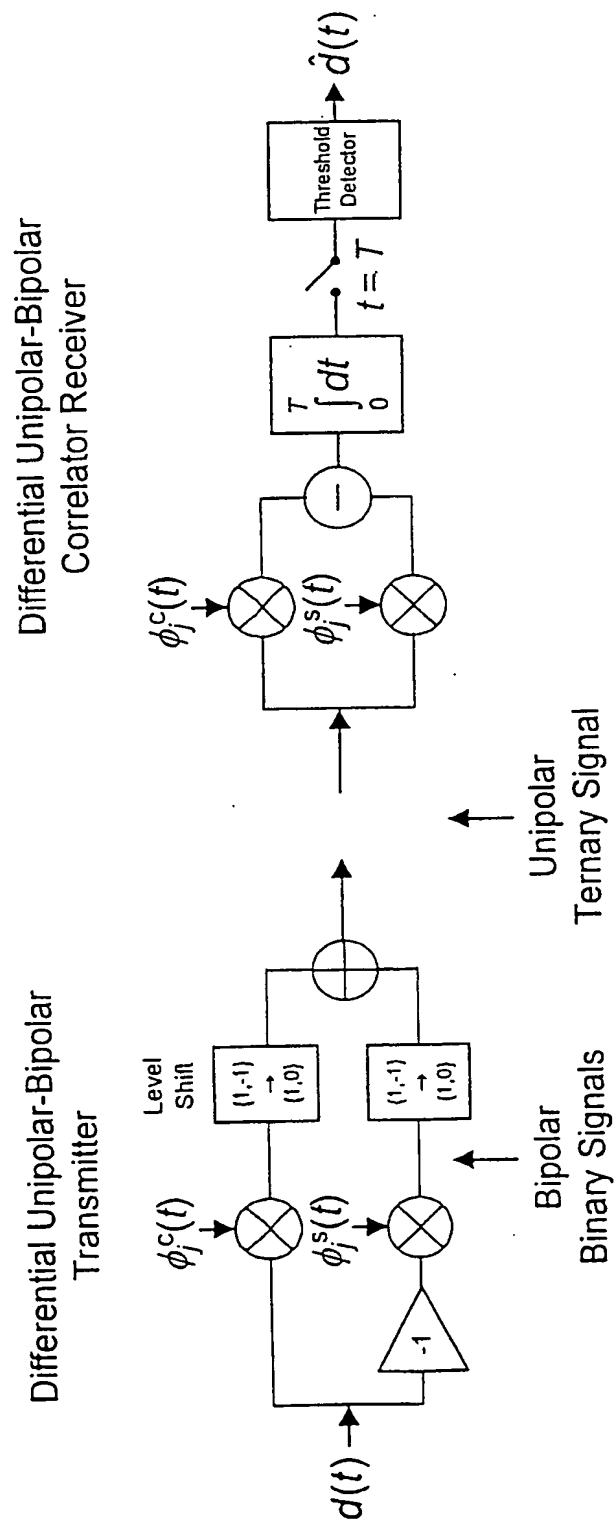


Figure 5

6/11

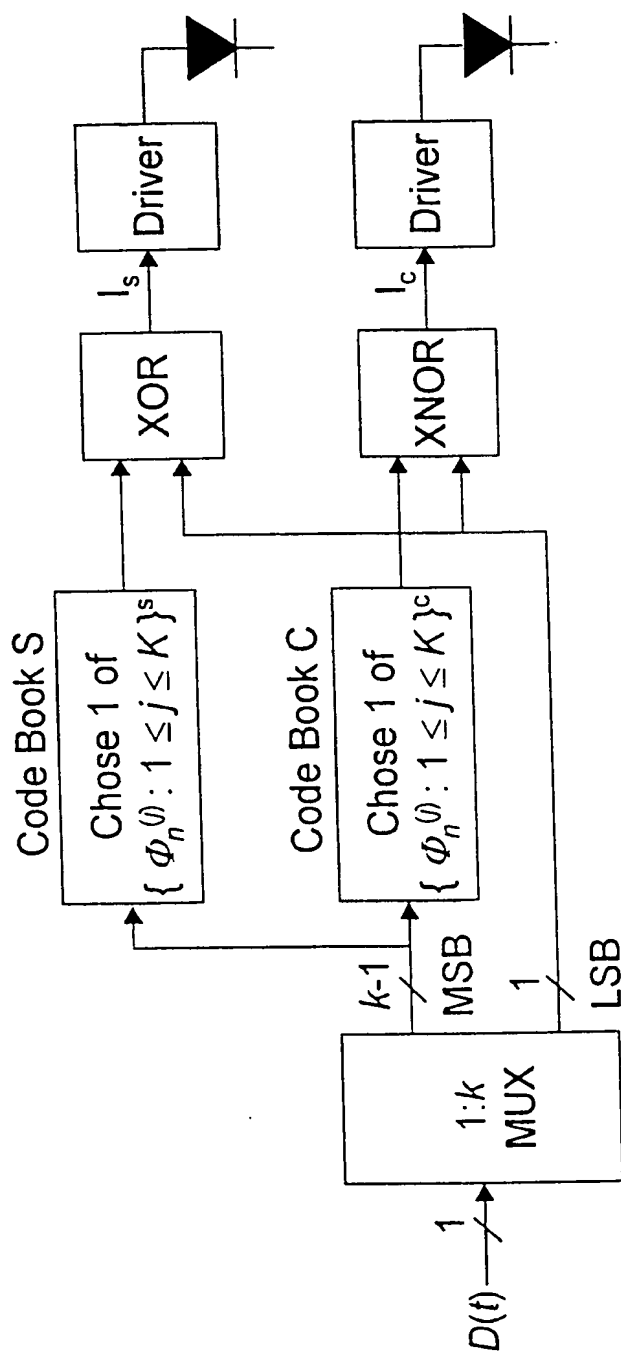


Figure 6

7/11

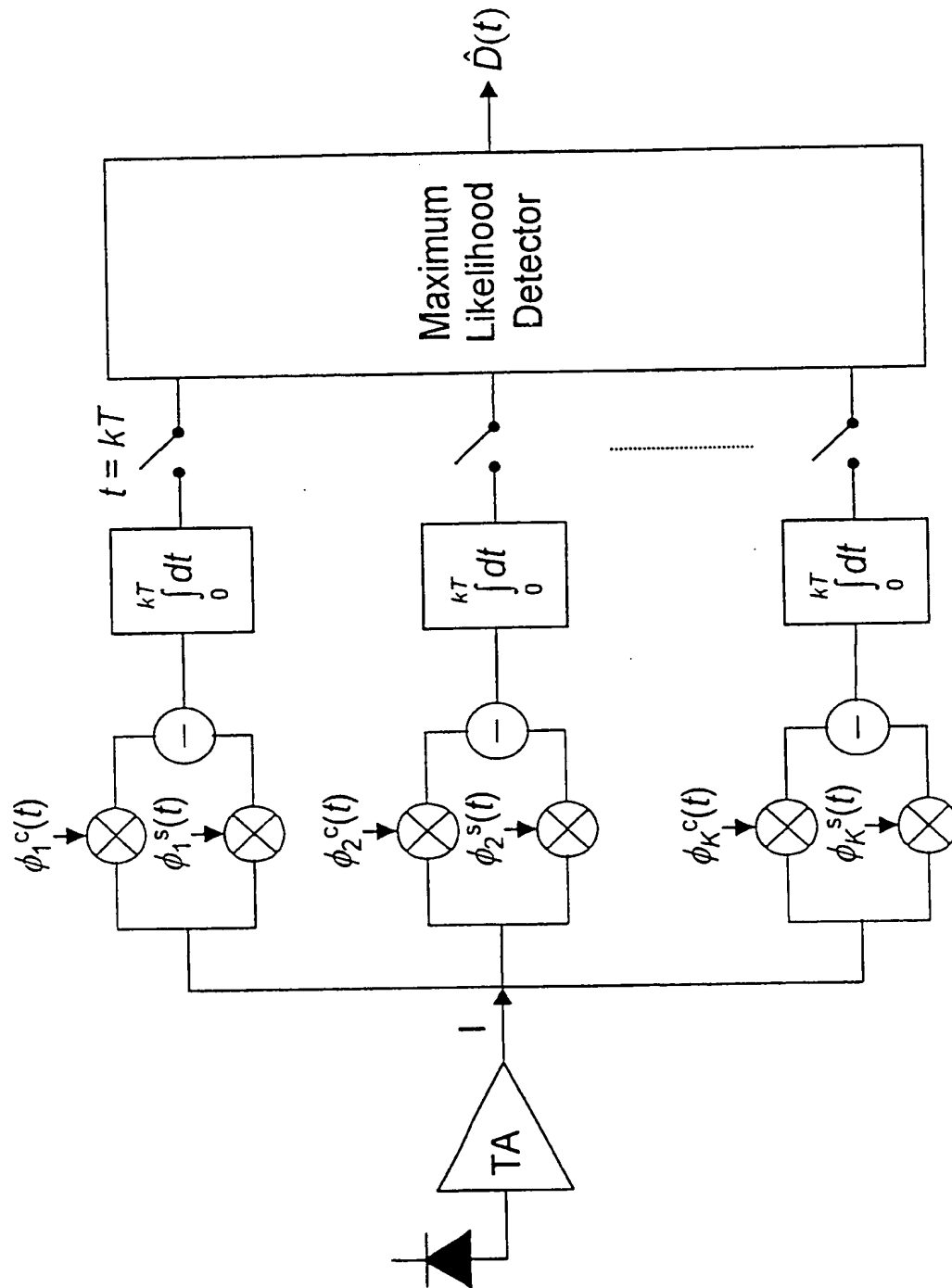


Figure 7

8/11

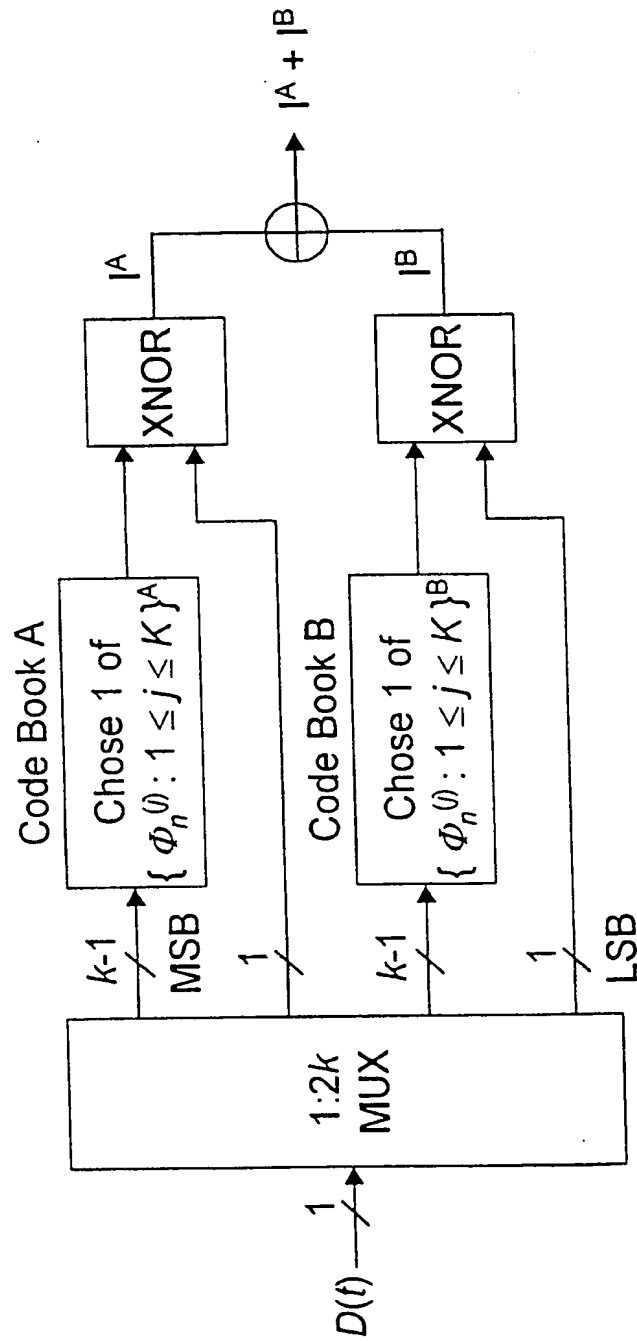


Figure 8

9/11

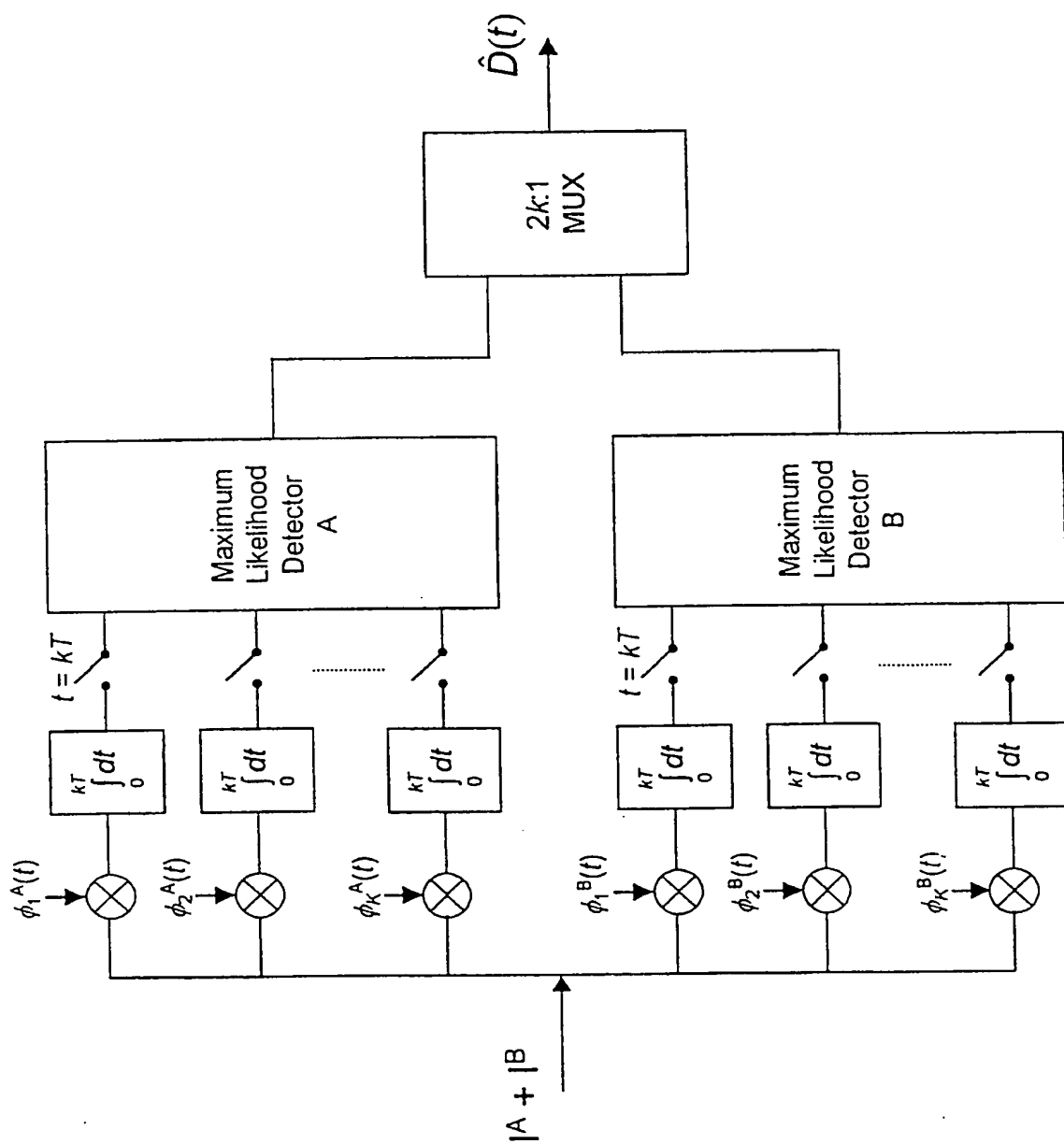


Figure 9

10/11

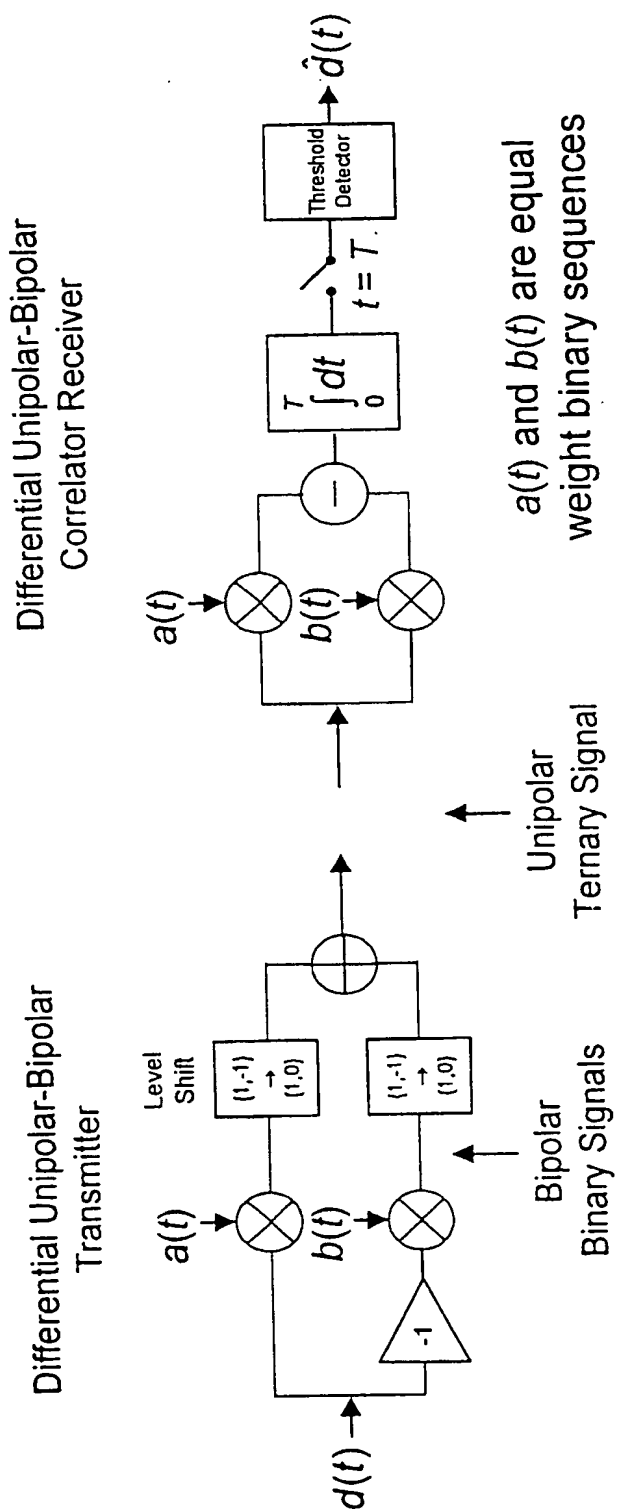
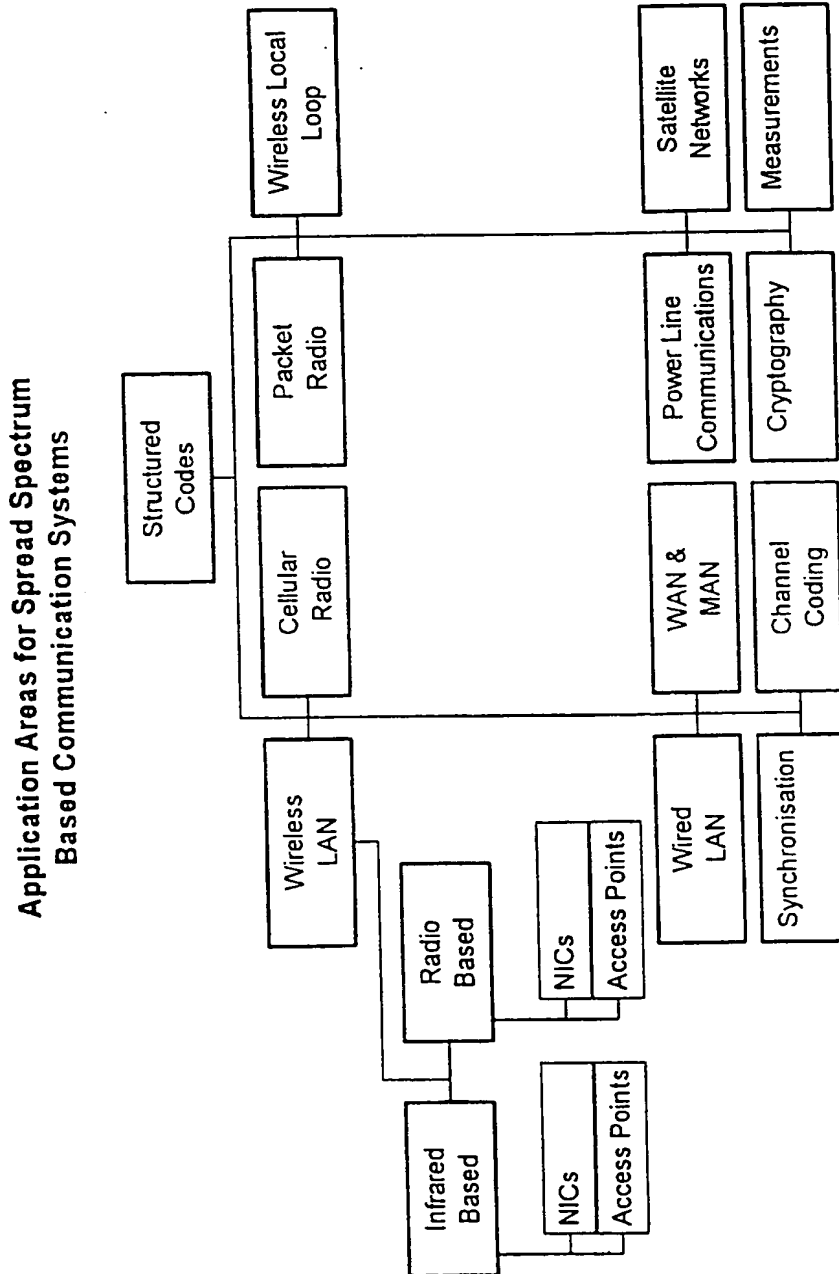


Figure 10

11/11

**Figure 11**

# INTERNATIONAL SEARCH REPORT

Intern. Appl. No.  
PCT/IE 98/00110

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 6 H04J13/00

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 6 H04J

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LE STRAT E: "NEW SPREADING CODES FOR A DS-CDMA MOBILE RADIO SYSTEM USING A RAKE RECEIVER IN A MULTI_USER INTERFERENCE ENVIRONMENT" IEEE ISSSTA'94, PROCEEDINGS OF IEEE 3RD INTERNATIONAL SYMPOSIUM ON SPREAD SPECTRUM TECHNIQUES AND APPLICATIONS, vol. 2, 4 - 6 July 1994, pages 401-405, XP002099155 OULU, FINLAND see abstract see part II	1-6, 11-17, 22-42
A	---	7,8,18, 19
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

8 April 1999

Date of mailing of the international search report

20/04/1999

Name and mailing address of the ISA  
European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Chauvet, C



# INTERNATIONAL SEARCH REPORT

Intern. Patent Application No  
PCT/IE 98/00110

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 559 829 A (LE STRAT E ET AL) 24 September 1996	1-6, 11-17, 22-42
A	see abstract see column 7, line 44 - column 10, line 2	7,8,18, 19
X	----- MO-HAN FONG ET AL: "CONCATENATED ORTHOGONAL/PN SPREADING SCHEME FOR CELLULAR DS-CDMA SYSTEMS WITH INREGATED TRAFFIC" COMMUNICATIONS - GATEWAY TO GLOBALIZATION. PROCEEDINGS OF THE CONFERENCE ON COMMUNICATIONS, SEATTLE, JUNE 18 - 22, 1995, vol. 2, 18 June 1995, pages 905-909, XP000533131 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS see abstract see part 1 see part 2.1 see part 3	1-6, 11-17, 22-42
A		7,8,18, 19
A	----- DAS J: "A TECHNIQUE FOR IMPROVING THE EFFICIENCY OF M-ARY SIGNALING" IEEE TRANSACTIONS ON COMMUNICATIONS, vol. COM-32, no. 2, February 1984, pages 199-201, XP002072640	1,12,23, 28,29
X	see the whole document -----	39-42

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. Appl. Application No

PCT/IE 98/00110

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5559829 A	24-09-1996	FR 2712444 A	19-05-1995
		AU 683694 B	20-11-1997
		AU 7752994 A	18-05-1995
		CA 2135459 A	11-05-1995
		CN 1124439 A	12-06-1996
		EP 0652647 A	10-05-1995
		FI 945230 A	11-05-1995
		JP 7202752 A	04-08-1995
		NZ 264805 A	26-11-1996
-----			